









<div><div>هيئة كهرباء ومياه دبي Dubai Electricity & Water Authority</div></div> <div>DEWA Contract No. RFX 2131600072</div>		<div>PROJECT NO: RFX 2131600072</div> <div>DESIGN, SUPPLY, INSTALLATION, TESTING & COMMISSIONING OF LOCAL SCADA SYSTEM ALONG WITH NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX</div>		<div><div>Silvertech Automation Contracting & Total Solutions</div></div> <div>Contractor's Project No.:PRJ212</div>
Current Transmittal No: PRJ212-TR-0083		COMMENT RESOLUTION SHEET-01		Previous Transmittal No.: PRJ212-TR-0035
Date of Transmittal: 30 July 2018				Document Approval Status: REVISE & RESUBMIT
DEWA Doc. No.: RFX72-DES-FDS		Document / Drawing Title: FUNCTIONAL DESIGN SPECIFICATION (FDS)		DEWA Review Reference: RFX72_RE 35
Revision No.: Rev 2				Date: 11 Jun 2018
Sl.No.	Document Section / Page	COMPANY Comments	Contractor Resolution	COMPANY Response
1.	-	Cybersecurity implementation guidelines based on assessment document and comprehensive Cyber security Network configuration plan, security & policy checklist.	To be provided as part of the <i>Cybersecurity FDS</i> . Document # <u>RFX72-CS-FDS</u> .	
2.	-	Data flow diagrams/logic diagrams between layer 1 & layer 2 via various Layer 2 & Layer 3 switches to be revealed as a part of the network configuration plan	To be provided as part of the <i>Cybersecurity FDS</i> . Document # <u>RFX72-CS-FDS</u> .	
3.	-	Access control system configuration detail, Functional Details & system architecture details along with the integration details to the SCADA system	Incorporated, detailed configuration and integration details to be provided as part of the <i>Software Design Specification</i> document # <u>RFX72-DES-SDS</u> .	
4.	-	NPM software implementation design for the network management, diagnostics & monitoring utilities including the design architecture and functionality details	To be provided as part of the <i>Cybersecurity FDS</i> . Document # <u>RFX72-CS-FDS</u> .	
5.	-	Final OCP	Final <i>Operational & Control Philosophy</i> document # <u>RFX72-Phase2-OCP</u> , to be updated based on DEWA discussion output of the meeting held on 16 th July 2018 for further submission.	
6.	-	Final design of the PLC panel, server cabinets to be included.	"Approved for construction" will be attached, Final revision "Post FAT" will be issued after FAT completion for any modification as required.	

<div><div>هيئة كهرباء ومياه دبي Dubai Electricity & Water Authority</div></div> <div>DEWA Contract No. RFX 2131600072</div>		<div>PROJECT NO: RFX 2131600072</div> <div>DESIGN, SUPPLY, INSTALLATION, TESTING & COMMISSIONING OF LOCAL SCADA SYSTEM ALONG WITH NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX</div>		<div><div>Silvertech Automation Contracting & Total Solutions</div></div> <div>Contractor's Project No.:PRJ212</div>
Current Transmittal No: PRJ212-TR-0083		<div>COMMENT RESOLUTION SHEET-01</div>		Previous Transmittal No.: PRJ212-TR-0035
Date of Transmittal: 30 July 2018				Document Approval Status: REVISE & RESUBMIT
DEWA Doc. No.: RFX72-DES-FDS				DEWA Review Reference: RFX72_RE 35
Revision No.: Rev 2		Document / Drawing Title: <div>FUNCTIONAL DESIGN SPECIFICATION (FDS)</div>		Date: 11 Jun 2018
Sl.No.	Document Section / Page	COMPANY Comments	Contractor Resolution	COMPANY Response
7.	-	SCADA system functionality including historian features and buffering of the data.	To be provided as part of the <i>Software Design Specification</i> document # <u>RFX-72-DES-SDS</u> .	
8.	-	Dream report configuration details, dashboard report developments including the interface details with SCADA system	To be provided as part of the <i>Software Design Specification</i> document # <u>RFX-72-DES-SDS</u> .	
9.	-	Reliability & Functionality of the system between PH 3 & PH 4 Cabinets for all the single source devices.	Incorporated, all single source devices were segregated between UPS & NON-UPS power supply for maximum availability as per approved <i>Internal Power Distribution Drawings</i> # <u>PRJ212-PH3-INS-PDD-0001</u> and <u>PRJ212-PH4-INS-PDD-0001</u>	
10.	-	Recoverability for the complete system including the detailed disaster recovery plan.	To be provided as part of the <i>Cybersecurity FDS</i> . Document # <u>RFX72-CS-FDS</u> .	
11.	-	Standards followed	Incorporated	
12.	-	Requirement analysis	To be provided as part of the <i>Cybersecurity FDS</i> . Document # <u>RFX72-CS-FDS</u> .	
13.	-	Project implementation guideline/ strategy with minimal shutdown for site commissioning.	It is part of <i>Commissioning and Changeover Method Statement for Najma Pumping Station SCADA</i> document # <u>RFX-COM-MOS</u> submitted on 28-Jun-18 via transmittal # TRS-0076	

<div><div>هيئة كهرباء ومياه دبي Dubai Electricity & Water Authority</div></div> <div>DEWA Contract No. RFX 2131600072</div>		<div>PROJECT NO: RFX 2131600072</div> <div>DESIGN, SUPPLY, INSTALLATION, TESTING & COMMISSIONING OF LOCAL SCADA SYSTEM ALONG WITH NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX</div>		<div><div>Silvertech Automation Contracting & Total Solutions</div></div> <div>Contractor's Project No.:PRJ212</div>
Current Transmittal No: PRJ212-TR-0083		COMMENT RESOLUTION SHEET-01		Previous Transmittal No.: PRJ212-TR-0035
Date of Transmittal: 30 July 2018				Document Approval Status: REVISE & RESUBMIT
DEWA Doc. No.: RFX72-DES-FDS		Document / Drawing Title: FUNCTIONAL DESIGN SPECIFICATION (FDS)		DEWA Review Reference: RFX72_RE 35
Revision No.: Rev 2				Date: 11 Jun 2018
Sl.No.	Document Section / Page	COMPANY Comments	Contractor Resolution	COMPANY Response
22.	-	Veritas configuration & backup plan	To be provided as part of the <i>Cybersecurity FDS</i> . Document # <u>RFX72-CS-FDS</u> .	
23.	-	Final control room layout details by stating as Najma 3 Control room (as primary control center) and Najma4 (Emergency center)	Included.	
24.	-	All STME document references to be revise as per the final approval document	Document reference/name to be used in the FDS , revision history to be traced via project EDR.	
25.	-	Client supplied document to be revise by including the PLC backup/SCADA backup provided as the database gathering inputs for new SCADA developments	Incorporated	
26.	-	Simulation test to be included as a part of the engineering services	Incorporated	
27.	-	Training contents and sessions to be revise as per the earlier discussions and agreement.	Incorporated	
28.	-	PLC backup/SCADA backup to be included as a client supplied data's as a database input for the new SCADA development	Incorporated	
29.	-	7.1 -> Redundant managed Ethernet switches should be included	Incorporated	

 <p>هيئة كهرباء ومياه دبي Dubai Electricity & Water Authority</p> <p>DEWA Contract No. RFX 2131600072</p>		<p>PROJECT NO: RFX 2131600072</p> <p>DESIGN, SUPPLY, INSTALLATION, TESTING & COMMISSIONING OF LOCAL SCADA SYSTEM ALONG WITH NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX</p>		 <p>Contractor's Project No.: PRJ212</p>
<p>Current Transmittal No: PRJ212-TR-0083</p>		<p>COMMENT RESOLUTION SHEET-01</p>		<p>Previous Transmittal No.: PRJ212-TR-0035</p>
<p>Date of Transmittal: 30 July 2018</p>				<p>Document Approval Status: REVISE & RESUBMIT</p>
<p>DEWA Doc. No.: RFX72-DES-FDS</p>		<p>Document / Drawing Title: FUNCTIONAL DESIGN SPECIFICATION (FDS)</p>		<p>DEWA Review Reference: RFX72_RE 35</p>
<p>Revision No.: Rev 2</p>				<p>Date: 11 Jun 2018</p>
Sl.No.	Document Section / Page	COMPANY Comments	Contractor Resolution	COMPANY Response
30.	-	13.0 -> 1/0 counts should be as per the actual site conditions based on the supplied backup, drawings.	Updated	
31.	-	14.3 to 14.7 should be as per the respective document approvals	Updated	
32.	-	16.1 to 16.2 should be as per the comments provided in GAD & IPWD	Updated	



PROJECT

RFX 2131600072

**Design, Supply, Installation, Testing & Commissioning of Local SCADA
System along with Network Security Implementation at Najma Pumping
Station Complex**

FUNCTIONAL DESIGN SPECIFICATION (FDS) (RFX72-DES-FDS-REV 1)

END USER



DUBAI ELECTRICITY & WATER AUTHORITY

SYSTEM INTEGRATOR





SILVERTECH MIDDLE EAST FZCO

Contractor Project No: PRJ212

Document No: PRJ212-CMN-INS-FDS-0001

1	29-Jul-18	Issued for Approval	Ayoosh Pillai	Nader Haj Hassan	Nader Haj Hassan	Ahmed Ayat
0	12-Feb-18	Issued for Review	Ayoosh Pillai	Nader Haj Hassan	Nader Haj Hassan	Ahmed Ayat
Rev	Date	Description	Prepared By	Checked By	Reviewed By	Approved By

	DESIGN, SUPPLY, INSTALLATION, TESTING & COMMISSIONING OF LOCAL SCADA SYSTEM ALONG WITH NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX		
PO: 3761700080	DEWA Doc No.: RFX72-DES-FDS	Contractor Doc No: PRJ212-CMN-INS-FDS-0001	Date: 29-Jul-2018
RFX - 2131600072	FUNCTIONAL DESIGN SPECIFICATION (FDS)		Rev: 1 Page 2 of 31

DOCUMENT CHANGE HISTORY

Rev.	Date of Issue	CR/DR Numbers	No. of Pages	Pages Changed and Reasons for Change
0	12-Feb-18	-	29 + ATT.	Initial Issue
1	29-Jul-18	DR-1	31 + ATT.	Issued for Approval

DISTRIBUTION LIST

Copy	Registered Holder
Master	SILVERTECH
Copy	DEWA

© Copyright 2018. SILVERTECH MIDDLE EAST FZCO. All Rights Reserved.

No part of this document may be used, translated into another language, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written consent of Silvertech Middle East FZCO.

While every effort has been made to ensure the accuracy of this document, Silvertech Middle East FZCO assumes no responsibility for omissions and errors. Neither is any liability assumed for damages resulting from the use of information contained herein.

Silvertech Middle East FZCO reserves the right to revise any information contained in this document without prior notice.

Questions or comment regarding this document or the product to which it relates should be directed to:

Silvertech ME FZCO
P.O. Box No. 17910,
Jebel Ali, Dubai,
UAE





	DESIGN, SUPPLY, INSTALLATION, TESTING & COMMISSIONING OF LOCAL SCADA SYSTEM ALONG WITH NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX		
PO: 3761700080	DEWA Doc No.: RFX72-DES-FDS	Contractor Doc No: PRJ212-CMN-INS-FDS-0001	Date: 29-Jul-2018
RFX - 2131600072	FUNCTIONAL DESIGN SPECIFICATION (FDS)		Rev: 1 Page 3 of 31

TABLE OF CONTENTS

1. PROJECT SUMMARY	5
1.1. PROJECT DESCRIPTION	5
1.2. PROJECT SCOPE.....	5
2. DEFINITIONS AND ABBREVIATIONS.....	6
3. REFERENCE DOCUMENTS AND STANDARDS	6
3.1. STANDARDS, CODES & REFERENCES.....	7
3.2. CLIENT SUPPLIED DOCUMENTS	8
3.3. STME DOCUMENTS.....	8
4. SCOPE OF THIS DOCUMENT.....	9
5. ENVIRONMENTAL REQUIREMENTS.....	9
6. POWER SUPPLY REQUIREMENTS	9
7. SCOPE OF SUPPLY	10
7.1. NAJMA PUMPING STATION (PHASE-3)	10
7.2. NAJMA PUMPING STATION (PHASE-4)	10
7.3. NAJMA PUMPING STATION (PHASE-2)	10
7.4. NAJMA PUMPING STATION (PHASE-1)	10
7.5. SUPPLY OF ASSET MANAGEMENT SYSTEM	11
7.6. SUPPLY OF PANEL ACCESS CONTROL SYSTEM	11
7.7. BILL OF MATERIALS	12
8. SCOPE OF SERVICES.....	14
8.1. SOFTWARE MODIFICATIONS ON PHASE-2 PLC SYSTEM.....	14
8.2. TRAINING.....	15
8.3. ENGINEERING SERVICES	15
9. EXISTING SYSTEM OVERVIEW	16
9.1. EXISTING SCADA SYSTEM OF NAJMA PUMPING STATION COMPLEX.	16
9.2. EXISTING PLC SYSTEM OF NAJMA PUMPING STATION COMPLEX.....	16
10. MODIFICATIONS AT NAJMA PUMPING STATION COMPLEX	17
11. SYSTEM HARDWARE SPECIFICATIONS.....	18
11.1. ENGINEERING WORK STATION.....	18
11.2. REDUNDANT APPLICATION SERVER.....	19
11.3. OPERATION WORK STATION.....	19
11.4. WSUS / MCAFEE EPO REPOSITORY SERVER.....	19
11.5. CYBER SECURITY HYPER-V SERVER	19
11.6. SCADA HYPER-V SERVER.....	20
11.7. OTHER COMPONENTS.....	21
12. SOFTWARE DETAILS	21
12.1. PLANTSTRUXTURE (PES) SCADA	21
12.2. VIJEO CITECT HISTORIAN.....	23

	DESIGN, SUPPLY, INSTALLATION, TESTING & COMMISSIONING OF LOCAL SCADA SYSTEM ALONG WITH NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX		
PO: 3761700080	DEWA Doc No.: RFX72-DES-FDS	Contractor Doc No: PRJ212-CMN-INS-FDS-0001	Date: 29-Jul-2018
RFX - 2131600072	FUNCTIONAL DESIGN SPECIFICATION (FDS)		Rev: 1 Page 4 of 31



12.3. REPORTING.....	23
12.4. ANTI-VIRUS AND SECURITY SOLUTION	23
12.5. BAKCUP EXEC	23
12.6. NETWORK PERFORMANCE MONITORING	23
13. PHASE -2 PLC I/O COUNTS.....	24
14. ENCLOSURE DESIGN AND CONSTRUCTION	24
14.1. SERVER CABINET SPECIFICATIONS	25
14.2. MAINTAINABILITY	25
14.3. PANEL POWER DISTRIBUTION AND PROTECTION.....	25
14.4. PANEL INTERNAL WIRING.....	26
14.5. WIRE COLOUR	26
14.6. WIRE SIZE.....	26
14.7. TRUNKING	27
14.8. SEGREGATION.....	27
14.9. TERMINATION OF MULTI-STRANDED WIRE.....	27
14.10. TERMINALS	27
15. POWER SUPPLY	28
16. IDENTIFICATION, LABELLING AND TAGGING	28
16.1. PANEL IDENTIFICATION	28
16.2. PANEL LABELLING.....	29
16.3. INTERNAL LABELLING AND TAGGING	29
16.4. WIRE IDENTIFICATION (FERRULING).....	30
17. INSPECTION AND TESTING	30
17.1. INTERNAL TEST	31
17.2. FACTORY ACCEPTANCE TESTS PROCEDURE	31
17.3. FACTORY ACCEPTANCE TESTS	31
17.4. SITE ACCEPTANCE TESTS PROCEDURE.....	31
18. DOCUMENTATION	31
19. PACKING, MARKING AND SHIPPING REQUIREMENTS	31

ATTACHMENT(S)

ATTACHMENT 1 – CATALOGUE AND DATASHEET

ATTACHMENT 2 – FACTORYTALK ASSET CENTRE CONFIGURATION GUIDELINE

ATTACHMENT 3 – CONTROL ROOM LAYOUT AND PANEL GENERAL ARRANGEMENT

	DESIGN, SUPPLY, INSTALLATION, TESTING & COMMISSIONING OF LOCAL SCADA SYSTEM ALONG WITH NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX		
PO: 3761700080	DEWA Doc No.: RFX72-DES-FDS	Contractor Doc No: PRJ212-CMN-INS-FDS-0001	Date: 29-Jul-2018
RFX - 2131600072	FUNCTIONAL DESIGN SPECIFICATION (FDS)		Rev: 1 Page 5 of 31

1. PROJECT SUMMARY

As a part of the DEWA strategic direction to enable its position as a “Sustainable innovative world – class utility”, it continuously evaluates its system to adopt its highest standards by implementing the cutting-edge technology practices.

The Dubai water transmission network comprises an extensive network of pipelines, pumping stations and reservoirs which convey the potable water from water production plants to water distribution system.

This contract pertains to the “Design, Supply, Installation, Testing and Commissioning of LOCAL SCADA System along with Network Security Implementation at Najma pumping station complex” which comprises of four phases within the complex itself.

The intent is to standardize on high quality of works throughout the project stage by aiming at achieving the objective of the business requirements.

1.1. PROJECT DESCRIPTION



Client	: Dubai Electricity & Water Authority (DEWA)
Contractor	: Silvertech Middle East (STME)
Project	: Design, Supply, Installation, Testing and Commissioning of Local SCADA System with Server –Client Architecture at Najma Pumping Station Complex
Location	: Dubai, UAE

1.2. PROJECT SCOPE

This project covers the design, supply, software program, configuration, factory testing, site installation, testing and commissioning of a new SCADA system at Najma Pumping Station Complex.

The main components of the project are:

- Design Engineering
- Audit of the SCADA system architecture by the OEM
- Design and audit of the ICS network security feature by the OEM
- Implementing cyber security features as per OEM recommendations and DEWA guidelines
- Re-engineering of the phase II PLC program as described in this document
- Supply of SCADA system as per the approved system architecture.
- Supply of IT Hardware’s including peripherals and other associated items.
- SCADA Design & Development using specified features with Phase 2 PLC.
- SCADA Design & Development using specified features with Phase 1, 3 & 4 PLC.
- Design and Application development of Historian Server software.

	DESIGN, SUPPLY, INSTALLATION, TESTING & COMMISSIONING OF LOCAL SCADA SYSTEM ALONG WITH NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX		
PO: 3761700080	DEWA Doc No.: RFX72-DES-FDS	Contractor Doc No: PRJ212-CMN-INS-FDS-0001	Date: 29-Jul-2018
RFX - 2131600072	FUNCTIONAL DESIGN SPECIFICATION (FDS)		Rev: 1 Page 6 of 31

- Design and development of Asset Management software.
- Design and supply of Control desks with civil works and necessary cabling.
- The supply of all necessary software and Hardware as outlined in this document.
- Technical training & Documentation
- Factory Acceptance Test
- Site Installation
- Site Acceptance Test / User Acceptance Test.



2. DEFINITIONS AND ABBREVIATIONS

DEWA	Dubai Electricity & Water Authority	EDR	Engineering Deliverables Register
HSE	Health, Safety & Environment	SAT	Site acceptance test
HSEMS	Health, Safety & Environment Management System	SCADA	Supervisory Control and Data Acquisition
AI	Analogue Input	STME	Silvertech Middle East
AO	Analogue Output	IO	Input / Output
CPU	Central Processing Unit	LAN	Local Area Network
DC	Direct Current	O/P	Output
DI	Digital Input	PLC	Programmable Logic Controller
DO	Digital Output	PSU	Power Supply Unit
FAT	Factory Acceptance Test	QA	Quality Assurance
FDS	Functional Design Specification	QC	Quality Control
GA	General Arrangement	UPS	Un-Interruptible Power Supply
HMI	Human Machine Interface		

3. REFERENCE DOCUMENTS AND STANDARDS



The system design has used the following documents for reference as applicable. Where there is a direct conflict, the order of precedence for Documents and Standards shall be as follows:

- Approved Technical Deviation / Concession Request
- This document – Functional Design Specification
- Approved Silvertech design documents
- Client Supplied Documents
- Applicable National and International Standards

	DESIGN, SUPPLY, INSTALLATION, TESTING & COMMISSIONING OF LOCAL SCADA SYSTEM ALONG WITH NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX		
PO: 3761700080	DEWA Doc No.: RFX72-DES-FDS	Contractor Doc No: PRJ212-CMN-INS-FDS-0001	Date: 29-Jul-2018
RFX - 2131600072	FUNCTIONAL DESIGN SPECIFICATION (FDS)		Rev: 1 Page 7 of 31

3.1. STANDARDS, CODES & REFERENCES

Instrument Society of America (ISA)	ISA – S5.1	Instrumentation symbols and identification
	ISA – S5.2	Binary Logic Diagrams for process operations
	ISA – S5.4	Instrument Loop Diagrams
	ISA-S71.01	Environmental Conditions for Process Measurement and Control Systems: Temperature and Humidity
	ISA-S71.02	Environmental Conditions for Process Measurement and Control Systems: Power
American Petroleum Institute (API)	ISA-S71.04	Environmental Conditions for Process Measurement and Control Systems: Airborne Contaminants
	API RP 551/2/4	Manual in Installation of Refinery Instruments and Control Systems
	API RP-14F	Recommended Practice for Design and Installation of Electrical Equipment for offshore Production Platforms.
	API RP554	Process Instrumentation and Control
Instrument Society of America (ISA)	ISA – S5.1	Instrumentation symbols and identification
	ISA – S5.2	Binary Logic Diagrams for process operations
	ISA – S5.4	Instrument Loop Diagrams
	ISA-S71.01	Environmental Conditions for Process Measurement and Control Systems: Temperature and Humidity
	ISA-S71.02	Environmental Conditions for Process Measurement and Control Systems: Power
American Petroleum Institute (API)	ISA-S71.04	Environmental Conditions for Process Measurement and Control Systems: Airborne Contaminants
	API RP-551/2/4	Manual in Installation of Refinery Instruments and Control Systems
	API RP-14F	Recommended Practice for Design and Installation of Electrical Equipment for offshore Production Platforms.
	API RP554	Process Instrumentation and Control
CENELEC Standards	EN 50081 (-2)	Electromagnetic Compatibility – Generic Emission Standard part 2: Industrial Environment
	EN 50082 (-2)	Electromagnetic Compatibility – Generic Immunity Standard part 2: Industrial Environment

	DESIGN, SUPPLY, INSTALLATION, TESTING & COMMISSIONING OF LOCAL SCADA SYSTEM ALONG WITH NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX		
PO: 3761700080	DEWA Doc No.: RFX72-DES-FDS	Contractor Doc No: PRJ212-CMN-INS-FDS-0001	Date: 29-Jul-2018
RFX - 2131600072	FUNCTIONAL DESIGN SPECIFICATION (FDS)		Rev: 1 Page 8 of 31



3.2. CLIENT SUPPLIED DOCUMENTS

S/N	DOCUMENT NO.	REV	DESCRIPTION
1	TENDER RFX 2131600072-Volume II		TECHNICAL SPECIFICATIONS
2	6121126010-PC01		PLC General Arrangement, Bill of materials and schematic wiring diagram - Phase I
3	6121126010-PC02		PLC General Arrangement, Bill of materials and schematic wiring diagram - Phase II
4	FW03200-03-DR01-WRD		Phase-3 PLC Panel Wiring Diagram
5	PRJ212-STME.P-DEWA-EG-TQR-0001 to 0011		DEWA reply for STME TECHNICAL QUERY
6	Client supplied data dated 27 September 201		PLC backup/SCADA backup

3.3. STME DOCUMENTS

S/N	DEWA DOC NO	STME DOC NUMBER	DESCRIPTION
1	RFX72-DES-SYS	PRJ212-CMN-INS-SBD-0001	System Architecture
2	RFX72-MAS-ITHW	PRJ212-CMN-INS-MAR-0001	SCADA Hardware Material Submittal
3	RFX72-MAS-Software	PRJ212-CMN-INS-MAR-0002	SCADA Software Material Submittal
4	RFX72-MAS-NWHW	PRJ212-CMN-INS-MAR-0003	Network Hardware Material Submittal
5	RFX72-DES-SYS	PRJ212-CMN-INS-SBD-0001	System Architecture
6	RFX72-SUR-RPT	PRJ212-CMN-SUR-RPT-001, 002 & 003	Site Survey Report
7	RFX72-CSMS-OEM	PRJ212-CMN-SYS-PHL-0001	Cyber Security Study by OEM

For the complete list of documents under this project please refer to Engineering Deliverables Register:
Doc No: RFX72-PM-EDR.

	DESIGN, SUPPLY, INSTALLATION, TESTING & COMMISSIONING OF LOCAL SCADA SYSTEM ALONG WITH NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX		
PO: 3761700080	DEWA Doc No.: RFX72-DES-FDS	Contractor Doc No: PRJ212-CMN-INS-FDS-0001	Date: 29-Jul-2018
RFX - 2131600072	FUNCTIONAL DESIGN SPECIFICATION (FDS)		Rev: 1 Page 9 of 31

4. SCOPE OF THIS DOCUMENT

Scope of this document is to define the system design principles and functionality. Where specific implementation methods or hardware components are required to meet the common hardware/software design philosophy, those items shall be specifically identified. Where many possible solutions or operating philosophies would satisfy the requirements, the Functional Design Specification defines the solution to be applied. The scope is to:

- Define the design principles and functionality of the system to be applied to meet the requirements
- Describe the hardware and software configuration of each element
- Define the make/models and quantities of major hardware component.

5. ENVIRONMENTAL REQUIREMENTS

Process Control System hardware non-operating conditions

Temperature: -30° to 60°C (-22° to 140°F).

Maximum rate of change of Temperature :20°C/hr (36°F/hr).

Humidity: 5% to 95% relative humidity (Rh), 38.7°C (101.7°F) maximum wet bulb temperature, non-Condensing.



Process Control System hardware operating conditions

Temperature: 10° to 35°C (50° to 95°F),

Humidity: Minimum to be the higher (more moisture) of -12°C (10.4°F) dew point or 8% relative humidity. Maximum to be the lower (less moisture) of 24°C (75.2°F) dew point or 90% relative humidity

6. POWER SUPPLY REQUIREMENTS

All systems shall be designed to operate from 240 VAC. Incomer feeder of 240 VAC power supply shall be made available by the client. Separate AC/DC convertor power supply is considered for the new managed switches and shall be accommodated to the respective PLC panel and server cabinet. Power Supply module should be capable of accepting a +/- 20% input voltage variation from nominal without shutting down (AC included).

	DESIGN, SUPPLY, INSTALLATION, TESTING & COMMISSIONING OF LOCAL SCADA SYSTEM ALONG WITH NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX		
PO: 3761700080	DEWA Doc No.: RFX72-DES-FDS	Contractor Doc No: PRJ212-CMN-INS-FDS-0001	Date: 29-Jul-2018
RFX - 2131600072	FUNCTIONAL DESIGN SPECIFICATION (FDS)		Rev: 1 Page 10 of 31

7. SCOPE OF SUPPLY

The scope of supply as per contract is listed in this section along with quantity for each item.

7.1. NAJMA PUMPING STATION (PHASE-3)

- Supply of main SCADA server.
- Supply of One (1) Primary Domain Controller server.
- Supply of Four (4) operator workstations with LED monitors.
- Supply of One (1) operator workstation connected to wall-mounted monitor.
- Supply of Redundant L3 Ethernet managed switches.
- Supply of Redundant Industrial managed Ethernet switches.
- Supply of Console furniture for housing the supplied operator workstations.
- Supply of One (1) server cabinet of dimensions 2000 x 800 x 1000 mm for housing the supplied servers and network equipment.
- Supply of standard cabinet accessories (ducts, terminals, trunking, wiring, ferrules, MCBs, etc.).
- Supply of One (1) KVM switch with retractable monitor and keyboard.

7.2. NAJMA PUMPING STATION (PHASE-4)



- Supply of disaster-recovery SCADA server.
- Supply of One (1) Historian and Asset Management server.
- Supply of One (1) Update Relay server.
- Supply of One (1) Cyber Security server.
- Supply of One (1) operator workstation with LED monitor.
- Supply of One (1) operator workstation connected to wall-mounted monitor.
- Supply of Redundant Ethernet managed switches.
- Supply of Redundant firewalls.
- Supply of One (1) server cabinet of dimensions 2000 x 800 x 1000 mm for housing the supplied servers and network equipment.
- Supply of standard cabinet accessories (ducts, terminals, trunking, wiring, ferrules, MCBs, etc.).
- Supply of One (1) KVM switch with retractable monitor and keyboard.

7.3. NAJMA PUMPING STATION (PHASE-2)

- Supply of Redundant Ethernet managed switches.

7.4. NAJMA PUMPING STATION (PHASE-1)

- Supply of Redundant Ethernet managed switches.

	DESIGN, SUPPLY, INSTALLATION, TESTING & COMMISSIONING OF LOCAL SCADA SYSTEM ALONG WITH NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX		
PO: 3761700080	DEWA Doc No.: RFX72-DES-FDS	Contractor Doc No: PRJ212-CMN-INS-FDS-0001	Date: 29-Jul-2018
RFX - 2131600072	FUNCTIONAL DESIGN SPECIFICATION (FDS)		Rev: 1 Page 11 of 31

7.5. SUPPLY OF ASSET MANAGEMENT SYSTEM

Supply of FactoryTalk® AssetCentre for 100 assets/instruments, a centralized tool for securing, managing, versioning, tracking and reporting automation-related asset information across entire Najma Pumping Station Complex. It will be installed on newly supplied SCADA server at Phase 4 Control room.

With FactoryTalk AssetCentre, the below will be achieved:

- Secure access to the system
- Track detailed users' actions
- Automatically track firmware versions
- Manage historical versioning of any electronic file
- Provide automatic backup and compare operations on supported devices

FactoryTalk® AssetCentre can be maintained, operated and monitored through one of the newly supplied operator workstations.



7.6. SUPPLY OF PANEL ACCESS CONTROL SYSTEM

The Access Control System CMCIII from Rittal shall be supplied for all phases and shall include a smart card reader with lock and centralized processing unit

Please refer to below CMCIII Bill of Material:

S/N	PART NUMBER	DESCRIPTION	QTY
1	7030010	CMCIII CMC Compact	4
2	7030000	CMC III Processing Unit	1
3	7030088	DK CMC III mounting units, 1 U	2
4	7030087	CMC III cable clamp straps	2
5	7030200	CMCIII CAN-Bus Unit Access	11
6	7320721	CMC-TC comfort handle for TS8 unit	9
7	7320700	Ergoform-S handle	2
8	7030230	CMCIII Transponder reader	7
9	2467000	Semi-cylinders for handle systems	11
10	7030071	Mounting unit	2
11	7030080	CMCIII Programming cable USB	1

The access will be configured for each area individually and save it at the main CPU for each cabinet. The access will be unique for front or rear door as per the required access and privileges provided by DEWA.

	DESIGN, SUPPLY, INSTALLATION, TESTING & COMMISSIONING OF LOCAL SCADA SYSTEM ALONG WITH NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX		
PO: 3761700080	DEWA Doc No.: RFX72-DES-FDS	Contractor Doc No: PRJ212-CMN-INS-FDS-0001	Date: 29-Jul-2018
RFX - 2131600072	FUNCTIONAL DESIGN SPECIFICATION (FDS)		Rev: 1 Page 12 of 31



Status and records for operation will demonstrated in the SCADA for each area and lock. Further detailed configuration to be provided as part of the *Software Design Specification* document # RFX-72-DES-SDS.

The access will be granted as below:



AREA		GROUP / USER	
		System Engineer	Operator
Phase 3 Server cabinet	Front	•	
	Rear	•	
Phase 4	Server cabinet	Front	•
		Rear	•
	PLC cabinet		•
	IO cabinet		•
Phase 1, PLC cabinet	Front	•	•
	Rear	•	
Phase 2, PLC cabinet	Front	•	•
	Rear	•	

7.7. BILL OF MATERIALS

A cumulative Bill of material is generated from the contractual requirements and tabulated below. This is tentative and for present reference and shall be updated on due course of the project engineering cycle.

	DESIGN, SUPPLY, INSTALLATION, TESTING & COMMISSIONING OF LOCAL SCADA SYSTEM ALONG WITH NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX		
PO: 3761700080	DEWA Doc No.: RFX72-DES-FDS	Contractor Doc No: PRJ212-CMN-INS-FDS-0001	Date: 29-Jul-2018
RFX - 2131600072	FUNCTIONAL DESIGN SPECIFICATION (FDS)		Rev: 1 Page 13 of 31

BILL OF MATERIAL				
S/N	DESCRIPTION	ITEM	MAKE	QTY
1	42U server rack (cable management kits, rack fan kits, Power distribution unit, with light kit	TS 5509.131	Rittal	2
2	Xeon CPU 2TB / 10 TB 16GB / 48GB RAM Windows Server 2012 R2 4 ports network port Redundant Power Supply 230V AC	PowerEdge R530	Dell	6
3	Xeon CPU 2TB HDD 16GB RAM Windows 10 Pro (64 bits) 4 ports network port Redundant Power Supply 230V AC	Precision 7920	Dell	1
4	Xeon CPU 2TB HDD 8GB / 16GB RAM Windows 10 Pro (64 bits) 4 ports network port Redundant Power Supply 230V AC	Precision 7910	Dell	6
5	27", Resolution 1920 x 1080 at 60 Hz Aspect ratio 16:9 Backlight LED DisplayPort 1.2, HDMI 1.4, VGA, 2 x USB 3.0 ,2 x USB 2.0	TBC	Dell	5
6	50inch, commercial grade Display	C501	NEC	2
7	Analog console switch, PS/2 & USB Support, 16 P port S/2, USB support	DAV2216-G01	Dell	2
8	18.5" console monitor 1366 x 768 WXGA	DKMMLED185-001	Dell	2
9	Aten KVM Extender remote and local unit	CE750A	ATEN	7
10	A4 color laser printer	M251n	HP	1
11	Smart Card locking system with log and user management.	CMC III	Rittal	1
12	Din rail Managed Ethernet Switch, 16 ports	TCSESM163F2CS0	Schneider Electric	8
13	Power Supply, 100-240 V AC / 24 V DC	QS20.244	Puls	2
14	1-U rack mounted, 24 ports, Managed Enterprise Ethernet Switch.	B5G124-24	Extreme	6

	DESIGN, SUPPLY, INSTALLATION, TESTING & COMMISSIONING OF LOCAL SCADA SYSTEM ALONG WITH NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX		
PO: 3761700080	DEWA Doc No.: RFX72-DES-FDS	Contractor Doc No: PRJ212-CMN-INS-FDS-0001	Date: 29-Jul-2018
RFX - 2131600072	FUNCTIONAL DESIGN SPECIFICATION (FDS)		Rev: 1 Page 14 of 31



S/N	DESCRIPTION	ITEM	MAKE	QTY
15	1-U rack mounted, 16 ports, Firewall.	SRX340	Juniper	2
16	Fiber Patch cords	Fiber Patch cords	Opterna/Comport	Lot
17	PES 4.3 (1250 objects)	EUSAPPCZSSPEZZ	Schneider Electric	1
18	Vijeo Citect Historian (15,000 points, 6 clients)	VJHNS211015	Schneider Electric	1
19	Energy Management Library	EUSEMLCZSSPEZZ	Schneider Electric	1
20	Reporting application (Unlimited tag, 15 clients)	CTDR11005	Dream Report	1
21	Antivirus	McAfee Endpoint Protection,	McAfee	1
22	Device Control Protection	McAfee DLP	McAfee	1
23	Host Intrusion Prevention	McAfee HIPS & ePO	McAfee	1
24	Asset Management Software	9515-ASTSRVREN	Rockwell Automation	1
25	SolarWinds Network Performance Monitor (SL100)	SolarWinds NPM	SolarWinds	1
26	Recovery software server, desktop & virtual edition	Backup Exec	Veritas	1

8. SCOPE OF SERVICES

8.1. SOFTWARE MODIFICATIONS ON PHASE-2 PLC SYSTEM

Re-engineering of the logic by considering the functional blocks of the SCADA and to avail the complete features of the PES SCADA system

- A complete auto operation of the plant shall be developed and implemented by considering the necessary logic modifications with reference to the discharge pressure and its relevant set point
- A complete simulation tests needs shall be demonstrated on the logic to test the complete scenarios and to confirm the satisfactorily plant operation. Simulation using SCADA coding and PLC simulation program needs to be carried out before the FAT.
- The control philosophy shall be developed by having the mutual discussion with the client as per the analyzed requirements.

	DESIGN, SUPPLY, INSTALLATION, TESTING & COMMISSIONING OF LOCAL SCADA SYSTEM ALONG WITH NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX		
PO: 3761700080	DEWA Doc No.: RFX72-DES-FDS	Contractor Doc No: PRJ212-CMN-INS-FDS-0001	Date: 29-Jul-2018
RFX - 2131600072	FUNCTIONAL DESIGN SPECIFICATION (FDS)		Rev: 1 Page 15 of 31

8.2. TRAINING

The training shall be at two levels with multi sessions to be conducted by OEM & STME.

The OEM will conduct two trainings:



- I. Basic SCADA functionality of PES on two sessions for maximum of 5 participants.
- II. Basic Introductory to Vijeo Historian on two sessions for maximum of 5 participants.

STME will conduct one training:

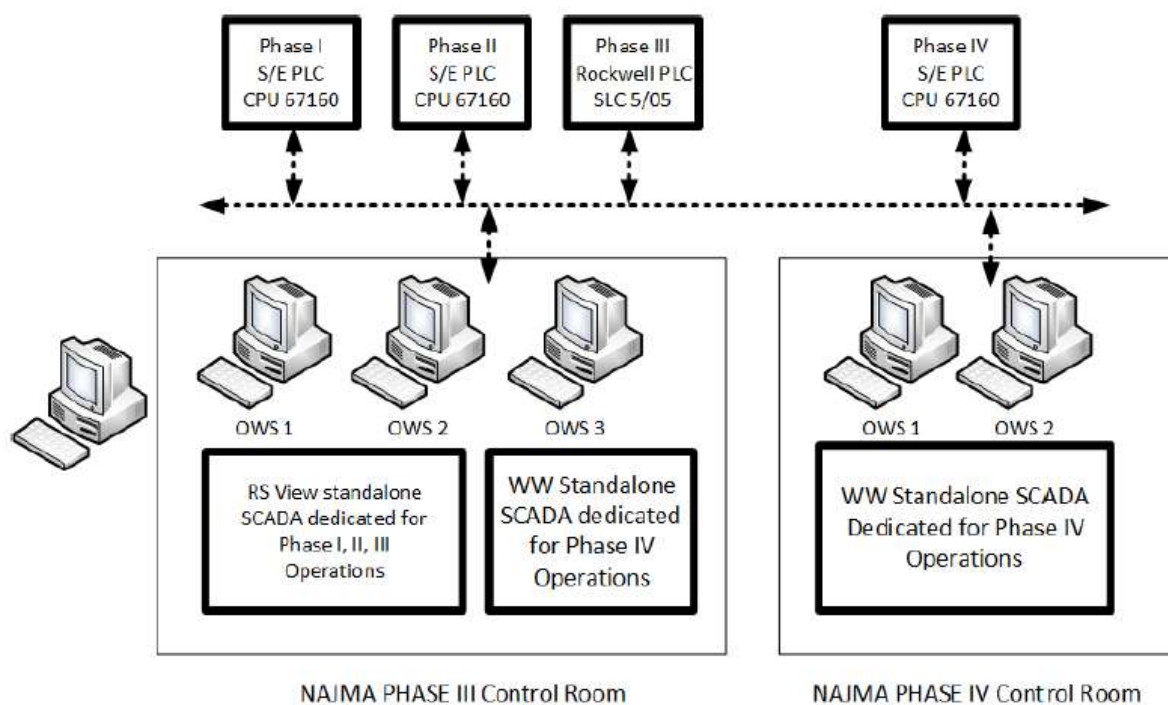
- I. Operation and maintenance covering all aspects on the efficiently using the SCADA .

8.3. ENGINEERING SERVICES

- Project Management Services
 - Project Management
 - Project Co-ordination and visits / meetings.
 - Quality Assurance
 - Administration services
- Project Engineering Services
 - Project Engineering
 - Hardware Engineering
 - Drawing Office
- System Functional Testing
 - Client witnessed Factory Acceptance Test with simulation test .
- System Documentation.
- Training.
- Installation, Pre-commissioning, Commissioning and Handover Services including reliability run test.

	DESIGN, SUPPLY, INSTALLATION, TESTING & COMMISSIONING OF LOCAL SCADA SYSTEM ALONG WITH NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX		
PO: 3761700080	DEWA Doc No.: RFX72-DES-FDS	Contractor Doc No: PRJ212-CMN-INS-FDS-0001	Date: 29-Jul-2018
RFX - 2131600072	FUNCTIONAL DESIGN SPECIFICATION (FDS)		Rev: 1 Page 16 of 31

9. EXISTING SYSTEM OVERVIEW





Existing system architecture of Najma pumping station complex

9.1. EXISTING SCADA SYSTEM OF NAJMA PUMPING STATION COMPLEX.

The existing SCADA system comprises of RS-View standalone SCADA dedicated for Phase-I, Phase-II and Phase-III operations and is stationed in the Phase 3 Control Room, and a dedicated Wonderware SCADA for Phase-IV operations with its operator stations distributed to both Phase-3 and Phase-4 Control rooms.

9.2. EXISTING PLC SYSTEM OF NAJMA PUMPING STATION COMPLEX

The SCADA system communicates with the control PLC of which Phase -I, Phase -II and Phase -IV are Schneider Electric Quantum range of PLC and the Phase-3 consist of Rockwell Automaton-PLC5 range of PLC.

	DESIGN, SUPPLY, INSTALLATION, TESTING & COMMISSIONING OF LOCAL SCADA SYSTEM ALONG WITH NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX		
PO: 3761700080	DEWA Doc No.: RFX72-DES-FDS	Contractor Doc No: PRJ212-CMN-INS-FDS-0001	Date: 29-Jul-2018
RFX - 2131600072	FUNCTIONAL DESIGN SPECIFICATION (FDS)		Rev: 1 Page 17 of 31



10. MODIFICATIONS AT NAJMA PUMPING STATION COMPLEX

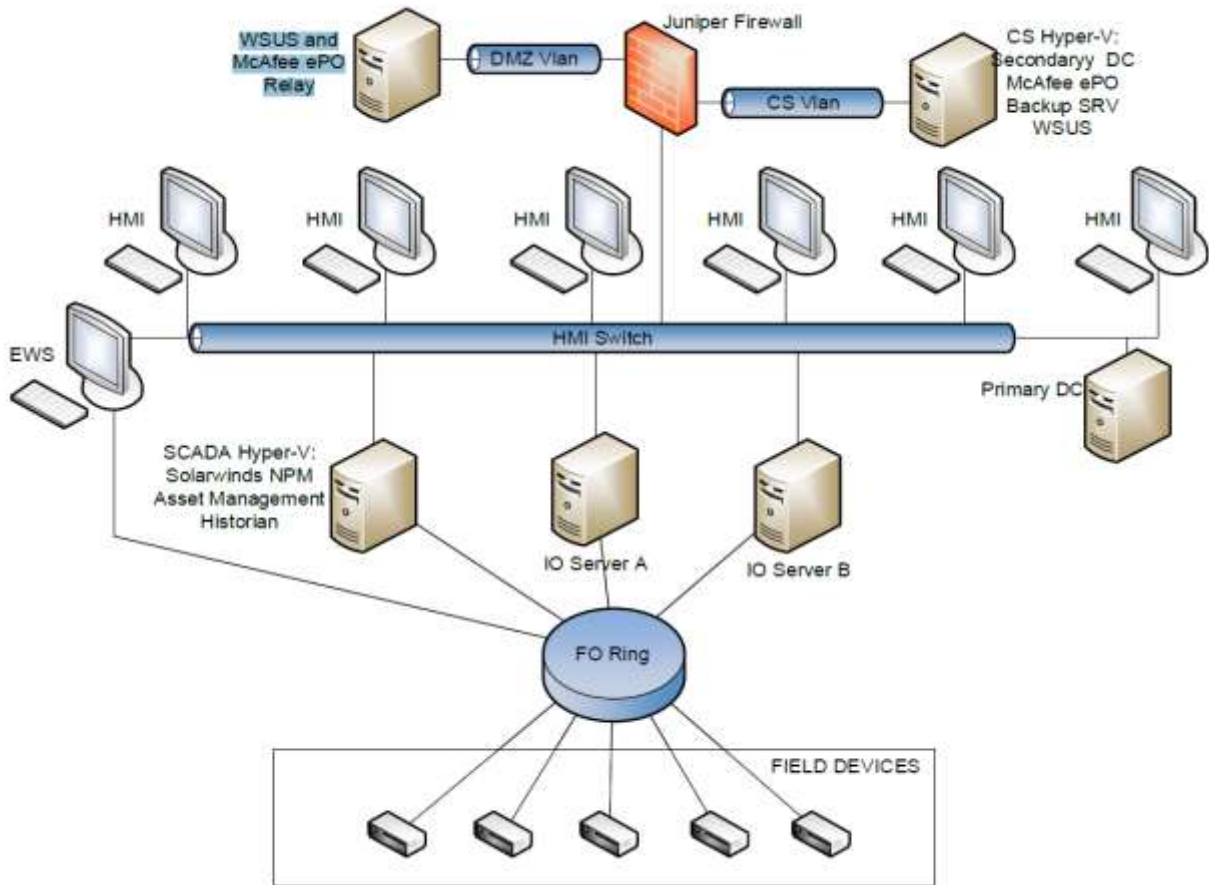
The main modification to be carried out as part of this upgrade is listed as below:

The operator stations shall be moved from the operator consoles to the server cabinet to provide physical security. Only KVM connections from the operator stations to the operator screens shall be provided. The PLC cabinets shall not be modified during this project; however, the Server and PLC cabinets shall be provided with access control via RFID card system. This is to provide physical security of the servers and switches in these racks.

Below showing detailed modification at each phase and function:

- Existing Phase 1 PLC to be integrated with new PES SCADA and Historian server.
- Existing Phase 2 PLC logic to re-developed and integrated with new PES SCADA and Historian server.
- Existing Phase 3 PLC to be integrated with new PES SCADA and Historian server.
- Existing Phase 4 PLC to be integrated with new PES SCADA and Historian server.
- Design and development of PES SCADA system with redundant application server, Historian servers and all other necessary arrangement.
- Asset Management System– Design and development of Asset management system and integration with 100 devices and equipment.

	DESIGN, SUPPLY, INSTALLATION, TESTING & COMMISSIONING OF LOCAL SCADA SYSTEM ALONG WITH NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX		
PO: 3761700080	DEWA Doc No.: RFX72-DES-FDS	Contractor Doc No: PRJ212-CMN-INS-FDS-0001	Date: 29-Jul-2018
RFX - 2131600072	FUNCTIONAL DESIGN SPECIFICATION (FDS)		Rev: 1 Page 18 of 31



SYSTEM ARCHITECTURE FOR AT NAJMA PUMPING STATION (With Server Applications Details)

11. SYSTEM HARDWARE SPECIFICATIONS



As shown in the figure above, the control system consists of the following distinct elements:

11.1. ENGINEERING WORK STATION

One number of dedicated engineering workstation is considered and shall be located at the phase-3 control room.

The Engineering station shall be hosting the below components.

- Core of the configuration
- Store applications and engineering tools for the PES.
- Enabling Runtime Services
- Mandatory to engineer / modify the deployed application

	DESIGN, SUPPLY, INSTALLATION, TESTING & COMMISSIONING OF LOCAL SCADA SYSTEM ALONG WITH NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX		
PO: 3761700080	DEWA Doc No.: RFX72-DES-FDS	Contractor Doc No: PRJ212-CMN-INS-FDS-0001	Date: 29-Jul-2018
RFX - 2131600072	FUNCTIONAL DESIGN SPECIFICATION (FDS)		Rev: 1 Page 19 of 31

11.2. REDUNDANT APPLICATION SERVER

The application servers are distributed to both the Phase-3 and Phase-4 Control room wherein the Phase -3 Control room shall host the primary application server and the Phase-4 one shall house the secondary with functions of IO data gathering, alarming, history and reporting.

The phase-4 Control room shall act as the disaster management control room with the secondary Application server, the Historian, Asset Management, cybersecurity servers, Backup and disaster recovery and the applications update servers. There are two domain controllers the primary and the secondary domain controller external to the PES hardware which is residing in servers at both Phase -III and Phase IV control room.

11.3. OPERATION WORK STATION

There are six operators work station out of which four shall be in phase 3 control room and two shall be in Phase-4 Control Room. One number of the OWS monitors in both control room shall be of 50 Inch Display and the others are 24 Inch configuration

- User interface for operators
- Entry point for runtime services
- Control client / view only client
- Local /remote & Web client

11.4. WSUS / MCAFEE EPO REPOSITORY SERVER

The Update Relay Server hosts the Windows server and Updated services(WSUS) and McAfee ePO updates relay. Windows server Updates and McAfee ePO updates are collected from the WAN through the update relay server. The Update Relay download security updates from the Active update servers directly through the WAN connection, and software updates from the Security Manager. When the relays are used, security and software updates only need to be downloaded once through the WAN connection. Relays then function as update distribution centers on the LAN, sending the security and software updates to the cyber security server which hosts the McAfee ePO and backup server. The Update relay servers are placed in the DMZ zones before the Juniper firewall and allows only the permitted data passage to the network and the updates are passed to the cybersecurity server for further storage in Remote storage devise.

11.5. CYBER SECURITY HYPER-V SERVER



The Cyber Security Server hosts the below applications:

1. WSUS

Centralized Windows Update server - enables administrators to manage the distribution of updates and hotfixes released for Microsoft products to computers in the SCADA

2. Backup Server

Centralized backup system – Collects and keeps copy of all backup files.

	DESIGN, SUPPLY, INSTALLATION, TESTING & COMMISSIONING OF LOCAL SCADA SYSTEM ALONG WITH NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX		
PO: 3761700080	DEWA Doc No.: RFX72-DES-FDS	Contractor Doc No: PRJ212-CMN-INS-FDS-0001	Date: 29-Jul-2018
RFX - 2131600072	FUNCTIONAL DESIGN SPECIFICATION (FDS)		Rev: 1 Page 20 of 31

3. McAfee ePO Server

Hosted in the cybersecurity server and gets updates from the relay server. It is Centralized Endpoint protection technology including Antivirus, Data Leak Protection, Host Intrusion Prevention and McAfee Agent

4. Secondary Domain Controller server

SDC acts as Active Directory Service in the network to perform Authentication, Authorization, Audit.

11.6. SCADA HYPER-V SERVER

This server hosts the below main applications:

1. VIJEO CITEC HISTORIAN SERVER

Vijeo Citect Historian comprises of historian and client functionalities, Citect Historian enables to accurately store data for long-term reporting while also giving the option of visualizing and accessing the information through the Citect Historian client, Microsoft Excel or Reporting Services. The Historian data shall be viewed on one of the operator work stations in both Phase-IV and Phase-III control room.

2. FACTORY TALK ASSET MANAGEMENT SERVER:



Factory Talk Asset Centre from Rockwell Automation provides a centralized tool for securing, managing, versioning, tracking and reporting automation-related asset information across the entire production system. And perhaps more importantly, it can do this automatically, with limited additional management oversight or work from employees.

- Source control leverages the centralized database and provides automatic version control.
- Audit trail consisting of Logged Time, Occurred Time, Source, Location, Resource, Username and Message.
- The Event logs consisting of Logged Time, Occurred Time, Source, Location, Severity and Message
- The reporting capabilities allow scheduled or on-demand searches that include traceability information from Audit, Events or Source Control.
- Standardized security model minimizes efforts to administer users and passwords on operator interfaces, historians, and engineering/ maintenance workstations.
- Asset Inventory Agent can automate discover and track the status of all connected devices, network switches and workstation computers across an entire facility or production operation.

Refer to *attachment 2* for FT Asset Centre configuration guide line.

3. NETWORK PERFORMANCE MONITORING:

Comprehensive Network Availability & Performance Monitoring and reporting for Multi- Vendor Networks - Monitor, track the up/down status, and analyze real-time, in-depth, network performance statistics for routers, switches, wireless access points, servers, virtualized environments and any other SNMP-enabled device through an intuitive web-based user interface that provides device-by-device drill down and detailed system information

	DESIGN, SUPPLY, INSTALLATION, TESTING & COMMISSIONING OF LOCAL SCADA SYSTEM ALONG WITH NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX		
PO: 3761700080	DEWA Doc No.: RFX72-DES-FDS	Contractor Doc No: PRJ212-CMN-INS-FDS-0001	Date: 29-Jul-2018
RFX - 2131600072	FUNCTIONAL DESIGN SPECIFICATION (FDS)		Rev: 1 Page 21 of 31

11.7. OTHER COMPONENTS

11.7.1. FIRE WALL

The connections from DMZ to the plant control network is restricted by redundant Juniper Fire walls SRX340 allows only pre-defined data exchange from outside the network for maximum protection.

11.7.2. ENTERPRISE SWITCHES

24 ports enterprise switches from Extreme B5G124-24 will be the core of communication between Najma Pumping Station servers & work stations with throughput 35.7 Mpps / 285.7 Mpps. The switches will be configured in redundant setup to achieve maximum availability.

For detailed data sheets for the above server applications and the IT hardware including the servers and work stations Refer *Attachment-1*.

12. SOFTWARE DETAILS



S/N	PART NUMBER	MAKE	DESCRIPTION
1	EUSBEUCZZSPEZZ	Schneider Electric	PlantStruxtre (PES) 4.3 ,1250 objects
2	VJHNS211015	Schneider Electric	Vijeo Citect Historian, 15,000 points & 6 clients
3	CTDR11005	Dream Report	Reporting application, Unlimited tag & 15 clients
4	CEBCDE-AA-AA	McAfee	McAfee Complete EndPoint Protection -Business: - Anti-Malware ENS - Device Control - HIP for Desktops
5	HISCDE-AB-AA	McAfee	Host Intrusion Prevention for Servers
6	13362-M0008 13132-M0008 11479-M0008	Veritas	Backup Exec
7	SL100	Solarwinds	Network Monitoring
8	9515-ASTSRVREN	Rockwell Automation	Asset Management Software
9	Office 2016	Microsoft	MS Office Licenses

12.1. PLANTSTRUXTURE (PES) SCADA

The proposed solution for the NAJMA pumping station upgrade is the Schneider electric PES V4.3.

The PES shall act as a single point software solution which can manage the control and supervisory elements for overall Najma pumping station which includes the Phase -I, Phase -II, Phase -III and Phase IV area.

Inside the PES environment Unity Pro and Vijeo Citect environment is used to configure the control and supervisory layers respectively with minimum engineering making use of the existing libraries.

	DESIGN, SUPPLY, INSTALLATION, TESTING & COMMISSIONING OF LOCAL SCADA SYSTEM ALONG WITH NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX		
PO: 3761700080	DEWA Doc No.: RFX72-DES-FDS	Contractor Doc No: PRJ212-CMN-INS-FDS-0001	Date: 29-Jul-2018
RFX - 2131600072	FUNCTIONAL DESIGN SPECIFICATION (FDS)		Rev: 1 Page 22 of 31



The Full PES features shall only be applicable in Phase -II section as the Phase -I, Phase -III and Phase -IV running PLC logic at shall not be modified. In view of above the Phase -2 Supervisory and Control configuration shall be done using the PES library. For the other Phases, the existing PLC logic shall be retained and re mapped to the supervisory layer which shall be now under Vijeo citec environment through PES. Effort shall be made to the maximum extent possible to have a similar appearance at least in the object level between the Phase-I, Phase II and Phase IV with Phase -II screens. However as there is no scope of modification in the PLC configuration for these phases there is limited flexibility for the above possibility.

The Faceplate features and other functionalities for these phases (Phase-I, Phase III and Phase IV) shall be limited to the existing configuration in general and any additional features or configuration contractually agreed.

The Phase -III PLC (Rockwell Automation PLC -5) shall be incorporated PES. It shall appear as an individual object inside the PES and can be communicated and the data can be channeled to the supervisory level for presentation to the operators in a uniform front end for the overall Najma Pumping station.

License selection was based on available objects in current SCADA and future expansion was taken in consideration. The selected objects tier was 1250; because it meets the minimum requirement and covering future expansions.

S/N	OBJECTS	QTY.
1	ANALYZER	32
2	FLOW TRANSMITTERS	17
3	PRESSURE TRANSMITTERS	65
4	VFD MOTORS	32
5	MCC FEEDER MONITORING	32
6	GENERATOR_MONITORING	8
7	MAINS_MONITORING	8
8	VFD MONITORING	32
9	VENTILATION SYSTEM	8
10	CHECK VALVES	30
11	MOTOR OPERATED VALVES (MODBUS)	124
12	UPS MONITORING	2
13	FIRE DERETECTION	4
14	FUEL OIL MANAGEMENT	3
15	MCC FEEDER MONITORING	1
16	GENRATOR MONITORING	1
Total counted objects		400
SYSTEM DIAGNOSTICS		100
MISCELLNEOUS Objects		100
SPARE 20%		120
Total object with 20%		720
LICENSE SELECTED		1250

	DESIGN, SUPPLY, INSTALLATION, TESTING & COMMISSIONING OF LOCAL SCADA SYSTEM ALONG WITH NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX		
PO: 3761700080	DEWA Doc No.: RFX72-DES-FDS	Contractor Doc No: PRJ212-CMN-INS-FDS-0001	Date: 29-Jul-2018
RFX - 2131600072	FUNCTIONAL DESIGN SPECIFICATION (FDS)		Rev: 1 Page 23 of 31

12.2. VIJEO CITECT HISTORIAN

Citect Historian provides an integrated long-term data archiving mechanism designed to store information from multiple disparate SCADA systems. The data store is an embedded Microsoft SQL Server 2 and can persist thousands of changes per second to the database. Connections to CitectSCADA control systems are made through the CitectSCADA interface CtApi, polling at a rate that is defined at each data source. Citect Historian acquires data from external SCADA systems via OPC V2 and OPC V3 Servers by subscribing to each tag and storing the changes. Data is stored in the database, along with meta-data describing the individual tag properties and quality for each sample.

12.3. REPORTING

The reporting application for Dream Reports is considered in the system which will enable report generation which is scheduled for a specific time of day, on a periodic basis, upon operator request, or event initiated (such as an alarm condition or end of batch). The system shall support printing to the designated report printer or to log all reports to a disk file or database (SQL, ODBC, DBF) or to a Web Server in a rich text file format such as HTML and shall have capacity to display the reports on to a screen. Reports shall support extensive calculations on both instantaneous and historical data, and any other data from the system.

12.4. ANTI-VIRUS AND SECURITY SOLUTION

With integrated, proactive security to combat sophisticated malware and zero-day threats, McAfee Endpoint Protection—Advanced Suite protects endpoints when they leave your network and helps protect your network when they return. Its integrated intrusion prevention secures desktops and servers from advanced threats. Centralized policy-based management, multiplatform support, and auditing keep all of your endpoint assets safe and compliant. The software will be deployed in the CyberSecurity server to be centralized point to manage all security related matter from one platform.

12.5. BACKUP EXEC



The proposed VERITAS Backup Exec delivers superior backup and disaster recovery for servers, desktops, and laptops with a single unified solution that enables businesses to recover from downtime or disasters in minutes. The backups will be stored in a dedicated server for any future requirements to retrieve it in any downtime.

Below editions will be used for each class machine as appropriate:

- 1- Backup Exec Server & Desktop Edition
- 2- Backup Exec V-Ray Edition

12.6. NETWORK PERFORMANCE MONITORING

SolarWinds Network Performance is a comprehensive Network Availability & Performance Monitoring and reporting for Multi Monitor, track the up/down status, and analyze real-time, in-depth, network performance statistics for routers, switches, wireless access points, servers, virtualized environments and any other SNMP-enabled device through an intuitive web-based user interface that provides device-by-device drill down and detailed system information. The NPM will be deployed in SCADA Hyper-V server and will be integrated with the PES SCADA for monitoring.

	DESIGN, SUPPLY, INSTALLATION, TESTING & COMMISSIONING OF LOCAL SCADA SYSTEM ALONG WITH NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX		
PO: 3761700080	DEWA Doc No.: RFX72-DES-FDS	Contractor Doc No: PRJ212-CMN-INS-FDS-0001	Date: 29-Jul-2018
RFX - 2131600072	FUNCTIONAL DESIGN SPECIFICATION (FDS)		Rev: 1 Page 24 of 31

13. PHASE -2 PLC I/O COUNTS

The below table indicated the number of hardwired I/O available in the Phase -II PLC.

DESCRIPTION	ACTUAL				TOTAL INCL. SPARE			
	DI	DO	AI	AO	DI	DO	AI	AO
Najma Pumping Station Phase-II PLC	176	32	46	8	224	48	96	16



The Supervisory Objects and Faceplates along with control function blocks, operator screen and navigation shall be listed under the detailed Software Design Specification (SDS) with document number RFX72-DES-SDS. For PES 4.3 application data sheet and catalogues please refer to *Attachment -1*

14. ENCLOSURE DESIGN AND CONSTRUCTION

The SCADA Systems hardware shall be housed in IP-55 rated cabinets from Rittal 5509.131 suitable for installation in indoor. The Panels shall be free standing in all the areas. More details are given below in this section. Access control is provided in the Cabinets to prevent unauthorized access to the hardware and to notify attempts for the same.

As part of the system cabinet/panel design, the following factors shall be considered:

- Structural rigidity
- Access for maintenance
- Separation of signal type and voltages
- Bend radius of cables
- Terminations
- Earthing
- Equipment & Wire labelling
- Ease of installation and Maintenance
- Installed Spares and Spare space

	DESIGN, SUPPLY, INSTALLATION, TESTING & COMMISSIONING OF LOCAL SCADA SYSTEM ALONG WITH NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX		
PO: 3761700080	DEWA Doc No.: RFX72-DES-FDS	Contractor Doc No: PRJ212-CMN-INS-FDS-0001	Date: 29-Jul-2018
RFX - 2131600072	FUNCTIONAL DESIGN SPECIFICATION (FDS)		Rev: 1 Page 25 of 31

14.1. SERVER CABINET SPECIFICATIONS

The panels are IP55 rated panels shall be used for all the cabinets. These panels have the following specifications. See *attachment 1* for data sheets of these panels.

PANEL'S SPECIFICATIONS	
Enclosure Type	Rittal Enclosure TS-IT – DK 5509.131
Enclosure Material	Mounting Plate 3mm thick sheet Steel
	Doors –2mm thick Sheet Steel (rear doors).
	Side/top Covers 1.5mm thick sheet steel
Dimensions:	Width: 800 mm Height: 2000 mm Depth: 1000 mm
Construction	42U
Color	Enclosure frame and panels: RAL 7035
IP Rating	IP 55 only in conjunction with baying seal or screw-fastened side panels
Access/Doors	Glazed Aluminum Door at the front and sheet steel rear door
Forced Cooling	Vent filter + Fan (top mounted) as per the air flow requirement
Cable Entry	Bottom

The cabinet shall be provided with tube panel lamp and an associated door switch. The cabinet shall have bottom access for the power and system cables. The cables shall be fixed to a removable type gland plate or shall be without glands depending upon client and site requirement. All internal power wiring for shall run through suitably sized PVC trunking.

14.2. MAINTAINABILITY



The design of the panels shall be such that it allows for easy maintenance, access to the components and testing. System shall be well laid out such that access to one item does not require the removal of another item. System components shall be secured using fasteners employing captive nuts or threaded holes, to facilitate easy installation or removal.

14.3. PANEL POWER DISTRIBUTION AND PROTECTION

This section describes the power supply distribution for the system. The incoming supplies are single UPS 230 VAC, 50 Hz and single non-UPS 230 VAC, 50 Hz.

The power for the new Ethernet switches shall be drawn from additional redundant AC/DC convertors. These convertors shall be installed inside the respective PLC panels of phase 1 , 2 & 4 and inside the server cabinets at Phase-3. All power supplies are rated for 70°C continuous operation. The 24V DC power shall be distributed by double pole circuit breakers. The 24 VDC output supply is floating earth type. The 24VDC feeds to individual field loads shall be using fused terminals.

The Utility loads shall be derived from the Incoming 230 VAC feeder Non -UPS power.

	DESIGN, SUPPLY, INSTALLATION, TESTING & COMMISSIONING OF LOCAL SCADA SYSTEM ALONG WITH NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX		
PO: 3761700080	DEWA Doc No.: RFX72-DES-FDS	Contractor Doc No: PRJ212-CMN-INS-FDS-0001	Date: 29-Jul-2018
RFX - 2131600072	FUNCTIONAL DESIGN SPECIFICATION (FDS)		Rev: 1 Page 26 of 31

14.4. PANEL INTERNAL WIRING

This section covers the selection and use of single core wires used inside the cabinet. Internal panel single core wire shall be tri rated sheathed, stranded, copper wire conductors. The wires used for internal wiring of the cabinet shall be flame retardant as per IEC 60332.

14.5. WIRE COLOUR

Panel internal wiring shall follow this colouring scheme based on the voltage levels they handle.



SIGNAL TYPE	COLOUR
24 VDC Supply	Blue
0 VDC Supply	Black
240 VAC Supply line (3 phase)	R : Red Y : Yellow B : Blue
240 VAC Supply Neutral	Black
Safety Earth	Green/Yellow
Instrument Earth	Plain Green

14.6. WIRE SIZE

Wire conductor size shall be determined in accordance with the circuit current and voltage drop requirements. The current carrying capacity and the length of the wire shall be determined during detailed design. As a minimum, the following wire and cable conductor sizes shall be used. However, wherever the current capacity is higher, then a wire of suitable size shall be used accordingly:

WIRE TYPE	MINIMUM SIZE
24 VDC Supply	1.0 - 1.5 mm ²
0 VDC Supply	1.0 - 1.5 mm ²
240 VAC Supply line	2.5 mm ² / 16 mm ²
240 VAC Supply Neutral	2.5 mm ² / 16 mm ²
Signal wiring	1.0 mm ²
Bonding Earth wire	4.0 mm ²

All wiring shall be one continuous length from terminal to terminal. Splicing shall not be permitted. All wiring connections shall be made using insulated crimp connectors.

	DESIGN, SUPPLY, INSTALLATION, TESTING & COMMISSIONING OF LOCAL SCADA SYSTEM ALONG WITH NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX		
PO: 3761700080	DEWA Doc No.: RFX72-DES-FDS	Contractor Doc No: PRJ212-CMN-INS-FDS-0001	Date: 29-Jul-2018
RFX - 2131600072	FUNCTIONAL DESIGN SPECIFICATION (FDS)		Rev: 1 Page 27 of 31

Wiring across door hinges shall be protected against mechanical damage by spiral and tie base if required.

14.7. TRUNKING

Panel wiring shall be loose laid in trunking with a retained cover. To allow for future expansion of the system, the trunking shall be sized to ensure that no more than 75% of the available space is used in the initial design. The trunking shall be flame retardant PVC material, GREY in colour. AC power shall be run within the panels in black trunking.

14.8. SEGREGATION

Internal panel 24VDC power and signal wiring shall be run in the grey trunking. AC power shall be segregated from all other wiring within the panels using black trunking.

AC input and output terminals shall be suitably protected using transparent terminal covers and warning labels (Hazardous marking with voltage level shall be provided).

All incoming field cabling shall be allocated a separate terminal group and a dedicated cable tray /trunking within the system panels.

The single source devices segregated between UPS and NON-UPS power supply to achieve maximum availability in case of power failure. Operation and functionality to be tested during FAT. Refer to Internal Power Distribution Drawings # PRJ212-PH3-INS-PDD-0001 and PRJ212-PH4-INS-PDD-0001 *Attachment 3* for Phase 3 & 4 server cabinets respectively for details.

14.9. TERMINATION OF MULTI-STRANDED WIRE

Wires with stranded conductors shall be terminated with insulated bootlace ferrules as standard. Where required, wires may be terminated with twin grip insulated crimps.

14.10. TERMINALS

DIN rail mounted screw type terminals selected from the Phoenix Contact range shall be used. Refer to *attachment 1*. Wherever terminals are to be linked, jumper or combing bars shall be used.



Power feed terminals shall be fused feed through terminals with fuse blown indication.

The use of more than two crimp connections per terminal position shall not be permitted. The use of looping wires shall be avoided to the maximum extended possible. Where the use of looping wires is required, the loop shall be fed at both ends.

The terminal sizes are as follows. However, wherever larger wire is required (based on the detailed calculation) then a terminal of suitable size shall be used accordingly:

230 AC Feeder Power Supply As per load calculation. Minimum of 4 sqmm.

Power Distribution 6.0 mm² / 2.5 mm²

	DESIGN, SUPPLY, INSTALLATION, TESTING & COMMISSIONING OF LOCAL SCADA SYSTEM ALONG WITH NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX		
PO: 3761700080	DEWA Doc No.: RFX72-DES-FDS	Contractor Doc No: PRJ212-CMN-INS-FDS-0001	Date: 29-Jul-2018
RFX - 2131600072	FUNCTIONAL DESIGN SPECIFICATION (FDS)		Rev: 1 Page 28 of 31

15. POWER SUPPLY

Each server cabinets will be supplied with Puls power supply QS20.244 20A to provide required power to ethernet switches and access control processor unit.

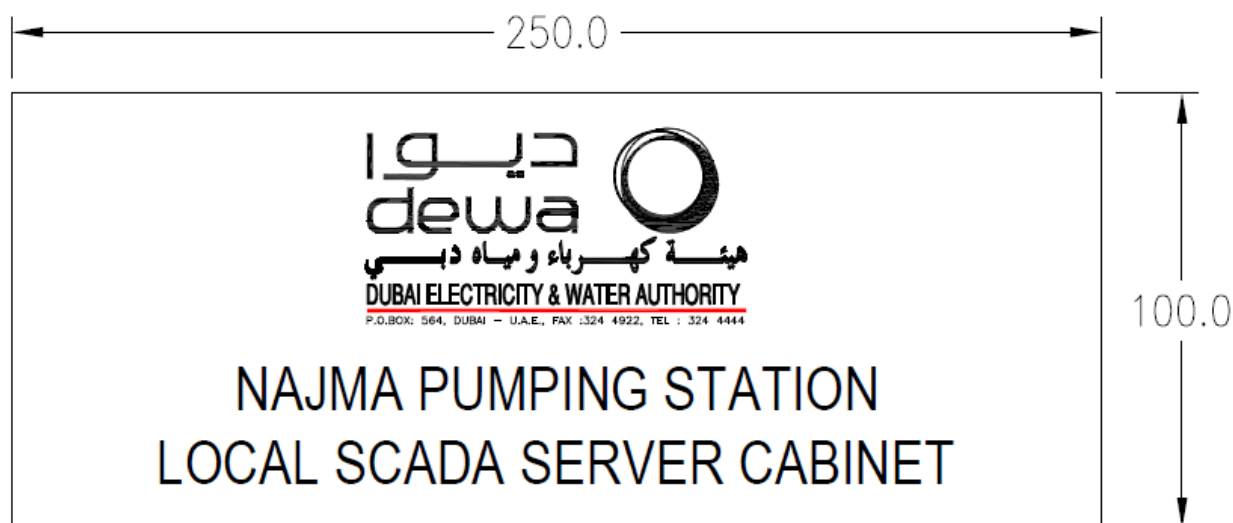
Please refer to the data sheet for further details.



16. IDENTIFICATION, LABELLING AND TAGGING

Each panel & each panel internal component shall be permanently identified with engraved nameplates as follows

16.1. PANEL IDENTIFICATION

The panels shall be equipped with a permanently attached primary nameplate manufactured from engraved stainless-steel plate/etched trifoliolate with black engraved lettering fixed with adhesive. It shall be fixed centred on the front door of each panel enclosure as indicated in example photo below.



	DESIGN, SUPPLY, INSTALLATION, TESTING & COMMISSIONING OF LOCAL SCADA SYSTEM ALONG WITH NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX		
PO: 3761700080	DEWA Doc No.: RFX72-DES-FDS	Contractor Doc No: PRJ212-CMN-INS-FDS-0001	Date: 29-Jul-2018
RFX - 2131600072	FUNCTIONAL DESIGN SPECIFICATION (FDS)		Rev: 1 Page 29 of 31

16.2. PANEL LABELLING

Manufacturer's (STME) label shall be an engraved stainless-steel label affixed by IP rated rivets. The dimensions of the label shall be 150(w) x 80(h) mm. One such label shall come per panel on the left most panel.



16.3. INTERNAL LABELLING AND TAGGING



Internal identification of major items shall be achieved using engraved trifoliate labels. Hazardous voltages shall be black on yellow; Safety and Instrument earth bars shall be white on green, and all others black on white.

Other labelling shall be achieved using paper, card or proprietary permanent labelling systems as applicable. All text shall be in upper case and of minimum size of 4mm where applicable.

For plug-in components, such as relays etc., an identification label shall be located on the mounting plate near the component and not on the component itself. Labels shall not be mounted on removable items such as the lids of trunking.

All equipment, plug-in cards, terminals, etc. shall be adequately identified and must have as a minimum the tag number with a shortened text.

If the panel is part of a bay the bay identification shall be the first letter in any label followed by an alphabetic sequence indicating the rail in each bay. Hence any component on the third panel in a bay and on the fifth rail shall start with CE. If it is a terminal group, it shall be named CE-TB01 to TB99. If it is a relay it shall be CE-K01 to K99

	DESIGN, SUPPLY, INSTALLATION, TESTING & COMMISSIONING OF LOCAL SCADA SYSTEM ALONG WITH NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX		
PO: 3761700080	DEWA Doc No.: RFX72-DES-FDS	Contractor Doc No: PRJ212-CMN-INS-FDS-0001	Date: 29-Jul-2018
RFX - 2131600072	FUNCTIONAL DESIGN SPECIFICATION (FDS)		Rev: 1 Page 30 of 31

Where applicable, multiple mounting locations within a bay shall be uniquely identified, for example as TR - Tray (swing-frame), TB - Terminal Bank, RL - Relay, CB - Circuit Breaker, with an additional identifier (A - Z) to be used as required. The position on a rail, plate or in a rack shall be identified as 01 to 99. The final termination identification shall be free format to allow for all forms of module location and termination.

The Terminal grouping shall also follow the cable schedule in such a way that each TB group is assigned to a Cable. Where ever Single pair and Two pair cables being there the Cable Tag shall be indicated by using integrated group Marker terminals or the Tags shall be fixed on the mounting plate.

16.4. WIRE IDENTIFICATION (FERRULING)

Cabinet single core wiring shall be identified black on white, permanently printed labels, identifying the termination location of the wire. Labels shall not be installed upside down. The wire shall be identified with both source and destination termination numbering. Ferrules shall be of transparent sleeve type with white inserts printed in black. Cross ferruling shall be followed in this project.

All wire cores shall be identified at both ends. The source termination numbers shall be always near to the terminating point regardless of the location / position of the component mounting. The above picture example using a FTA (Field Termination Assembly) shows the wire ferruling philosophy

FTA Side:

If termination is on the right-hand side or top side of the FTA.

<FTA Terminal No.>-<FTA TB Name>-<FTA Location> / <TB ID>-<Terminal No.>

If termination is on the left-hand side (as in above example) or bottom side of the FTA.

<TB ID>-<Terminal No.> / <FTA Location>-<FTA TB Name>-<FTA Terminal No.>

In the above example the ferrule is 01-TB11/LB01-TB1-01

Field TB Side:

If the panel internal wire termination is on the right-hand side or top side of the terminal block.

<Terminal No.>-<TB ID> / <FTA location>-<FTA TB name>-<FTA Terminal No.>

e.g. 01-TB11/LB01-TB1-01



If the panel internal wire termination is on the left-hand side of the terminal block.

<FTA Terminal No.>-<FTA TB Name>-<FTA Location> / <TB ID>-<Terminal No.>

e.g. 01-TB1-LB-03/TB21-01

17. INSPECTION AND TESTING

The inspection and testing shall be carried out over stages which shall cover the in-house inspection and testing carried out by STME and Factory Acceptance Testing (FAT) as part of this scope. However, STME support shall be provided for Installation Supervision, Integrated FAT, Commissioning and Site Acceptance Testing on man-day rate basis as required.

	DESIGN, SUPPLY, INSTALLATION, TESTING & COMMISSIONING OF LOCAL SCADA SYSTEM ALONG WITH NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX		
PO: 3761700080	DEWA Doc No.: RFX72-DES-FDS	Contractor Doc No: PRJ212-CMN-INS-FDS-0001	Date: 29-Jul-2018
RFX - 2131600072	FUNCTIONAL DESIGN SPECIFICATION (FDS)		Rev: 1 Page 31 of 31

FAT for the Najma System upgrade Scada including software simulation shall be conducted at STME premises at Jebel Ali Free Zone - Dubai.

17.1. INTERNAL TEST

STME shall carry out all the required internal tests for the hardware and the application software. All the internal test results shall be recorded and these records such as the internal test procedure, test result log, and corrective action taken shall be submitted to DEWA for their review.

STME shall undertake the FAT only after completing the internal tests successfully.

17.2. FACTORY ACCEPTANCE TESTS PROCEDURE

FAT procedure shall be prepared by STME and submitted for approval.

17.3. FACTORY ACCEPTANCE TESTS

A detailed FAT procedure shall be prepared by STME and submitted for approval. The Factory Acceptance Tests shall be conducted in accordance with approved procedure.

During FAT, 100% simulation of all I/O's and communication tests shall be carried out.

All records shall be verified and signed by client.

17.4. SITE ACCEPTANCE TESTS PROCEDURE

SAT procedure shall be prepared by STME and submitted for approval.

The site acceptance test shall repeat all test / functions tested during FAT while the system is installed and connected and interfaced to the field devices or the other systems.

During SAT, the complete operation philosophy for the system shall be checked with actual field equipment's connected.

All records shall be verified and signed by client.

18. DOCUMENTATION



STME shall generally supply drawings and documentation as identified in the vendor document requirements list to meet the requirements of DEWA

Refer: Engineering Deliverables Register RFX72-PM-EDR for more details.

19. PACKING, MARKING AND SHIPPING REQUIREMENTS

All equipment shall be packaged as per best practices to avoid any damage due to shock, vibration, rust, fungi, bacterial growth and dust or moisture ingress.

All crates and packages shall be clearly labelled and inventoried. STME shall provide a detailed packing list for each crate/package shipped.

	DESIGN, SUPPLY, INSTALLATION, TESTING & COMMISSIONING OF LOCAL SCADA SYSTEM ALONG WITH NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX		
PO: 3761700080	DEWA Doc No.: RFX72-DES-FDS	Contractor Doc No: PRJ212-CMN-INS-FDS-0001	Date: 29-Jul-2018
RFX - 2131600072	FUNCTIONAL DESIGN SPECIFICATION (FDS)		Rev: 1 Attachment-1

ATTACHMENT 1 – CATALOGUE AND DATASHEET

ATTACHMENT 1 – CATALOGUE AND DATASHEET

SCADA

Rittal – The System.

Faster – better – everywhere.



TS-IT – DK 5509.131

Date : 2017.11.08

ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

IT INFRASTRUCTURE

SOFTWARE & SERVICES

FRIEDHELM LOH GROUP



TS-IT – DK 5509.131

created: 08.11.2017 build on www.rittal.com/hr-hr



Product description

Material:	Čelični lim
Surface finish:	Enclosure frame: Dipcoat-primed Interior installation: Dipcoat-primed Doors and roof: Dipcoat-primed, powder-coated
Colour:	Enclosure frame and panels: RAL 7035 Interior installation: RAL 9005
Protection category IP to IEC 60 529:	IP 55 only in conjunction with baying seal or screw-fastened side panels
Supply includes:	TS 8 enclosure frame with doors and roof plate Glazed aluminium door at the front, 180° hinges Sheet steel door at the rear, 180° hinges Lock front and rear: Comfort handle for semi-cylinders and security lock 3524 E Roof plate, one-piece, solid Base tray and gland plate, multi-piece, solid Two 482.6 mm (19") mounting frames, front and rear, depth-variable Baying seal and sealing kit for gland plates (supplied loose) Connection accessories for potential equalisation with earthing point (supplied loose) 50 multi-tooth screws M5, cage nuts M5, conductive (supplied loose) IPPC pallet
Note:	Depending on how and where it is sited, the door opening angle may vary for selected applications For enclosures with height and depth 2000 x 1200 mm / 2200 x 1000 mm / 2200 x 1200 mm, the matching side panels are optionally available and are supplied fitted to the enclosure
Basic material:	Čelični lim

Product features

Dimensions:	Width: 800 mm Height: 2000 mm Depth: 1000 mm
Installation height for components:	42 U
Distance between levels as delivered:	745 mm
482.6 mm (19") version:	Montažni okvir, 482,6 mm (19")
Construction doors:	Sealed, IP 55
Load capacity:	10000 N
Packs of:	1 pc(s).
Weight/pack:	134,8 kg
EAN:	4028177705777
Customs tariff number:	94032080
ETIM 6.0:	EC002499
ETIM 5.0:	EC002499
eCl@ss 8.0/8.1:	27180207
eCl@ss 7.0/7.1:	27180207
eCl@ss 6.0/6.1:	27180207
eCl@ss 5.1/5.1.4:	27180201
Product description (long):	DK Network/server enclosure TS IT, with 19" mounting frame, WHD: 800x2000x1000 mm, 42 U, IP 55, Glazed aluminium door at the front, Sheet steel door at the rear, 180° hinges,
Approvals	
Approvals:	UL + C-UL
Certificates:	Protection category
Declarations:	Declaration of conformity



POWEREDGE R530

Versatile and affordable two-socket, 2U mainstream rack server delivers balanced performance and mid-range scalability for a wide range of common business workloads.

Designed for data centers needing an affordable, virtualization-ready, two-socket rack server, the PowerEdge R530 is an excellent platform for a wide range of common business applications and small-scale virtualization. The R530 is also highly attractive as a dedicated development or backup server.

Deliver powerful performance

Accelerate performance across a wide range of workloads with the latest Intel® Xeon® processor E5-2600 v4 product family. Drive greater memory performance with 12 DIMM slots and DDR4 memory. Boost I/O performance with five PCIe slots, including three PCIe 3.0 slots driving 2x data throughput compared to the previous generation.

Maximize operational efficiency

Accelerate time to production and drive better ROI by automating deployment with the embedded integrated Dell Remote Access Controller 8 (iDRAC8) with Lifecycle Controller. Save time for IT administrators with intuitive automated tools for monitoring and updating. Control energy budgets with highly energy-efficient processors, memory, power supplies and Fresh Air 2.0 capability.

Discover greater versatility

Easily accommodate data growth with support for up to 8 x 3.5" hard drives. Select from a range of RAID options for data protection and optimized performance. Adapt flexibly to changing workload conditions with an expandable platform ready for virtualization and high-availability clustering.

Innovative management with intelligent automation

The Dell OpenManage systems management portfolio includes innovative solutions that simplify and automate essential server lifecycle management tasks — making IT operations more efficient and Dell servers the most productive, reliable and cost effective. Leveraging the incomparable agent-free capabilities of the PowerEdge embedded iDRAC with Lifecycle Controller technology, server deployment, configuration and updates are streamlined across the OpenManage portfolio and through integration with third-party management solutions.

Monitoring and control of Dell and third-party data center hardware is provided by OpenManage Essentials and with anytime, anywhere mobile access, through OpenManage Mobile. OpenManage Essentials now also delivers Server Configuration Management capabilities that automate one:many PowerEdge bare-metal server and OS deployments, quick and consistent replication of configurations and ensure compliance to a predefined baseline with automated drift detection.

PowerEdge R530

- Latest Intel Xeon processor E5-2600 v4 product family
- Up to 12 x DDR4 DIMMs
- Up to 8 x 3.5" hard drives
- Up to 5 x PCIe slots (including 3 x PCIe 3.0)

Feature	Technical specification	
Form factor	2U rack server	
Dimensions and weight	H: 86.80 mm (3.4 in) W: 434 mm (17.1 in) without ears D: 646 mm (25.4 in) with bezel, 648 mm (25.5 in) without bezel	Minimum weight: 14.2 kg (31.2 lb) Maximum weight: 28.2 kg (62 lb)
Processor	Intel® Xeon® processor E5-2600 v4 product family Processor sockets: 2 Chipset: C610 Internal interconnect: up to 9.6GT/s; Cache: 2.5MB per core; core options: 4, 6, 8, 10, 12, 14, 16, 18	
Memory	DDR4 DIMMs at up to 2400MT/s; 12 DIMM slots: 4GB/8GB/16GB/32GB	
I/O slots	Support for up to 5 x PCIe • 3 x PCIe 3.0 • 2 x PCIe 2.0	
Storage	Up to 8 x 3.5" SAS, SATA, nearline SAS, SSD drives	
RAID controllers	Internal controllers: PERC S130 (SW RAID), PERC H330, PERC H730, PERC H730P External HBAs (RAID): PERC H830 External HBAs (non-RAID): 12Gbps SAS HBA	
Communications	4 x 1GbE LOM Click here for R530 supported network interface cards (NICs) and host bus adapters (HBAs) and scroll to "Additional Network Cards" section.	
Power supplies	495W, 750W, 1100W hot-plug PSU; -48V DC 1100W hot-plug PSU; 450W cabled PSU..	
Systems management	Systems management: IPMI 2.0 compliant; Dell OpenManage Essentials; Dell OpenManage Mobile; Dell OpenManage Power Center Remote management: iDRAC8 with Lifecycle Controller; iDRAC8 Express (default); iDRAC8 Enterprise (upgrade); 8GB vFlash media (upgrade); 16GB vFlash media (upgrade)	Dell OpenManage Integrations: • Dell OpenManage Integration Suite for Microsoft® System Center • Dell OpenManage Integration for VMware® vCenter™ Dell OpenManage Connections: • HP Operations Manager, IBM Tivoli® Netcool® and CA Network and Systems Management • Dell OpenManage Plug-in for Oracle® Database Manager
Optional supported hypervisors	Citrix® XenServer, VMware vSphere® ESXi®, Red Hat® Enterprise Virtualization	
Operating systems	Microsoft Windows Server® 2008 R2 Microsoft Windows Server 2012 Microsoft Windows Server 2012 R2 Novell® SUSE® Linux Enterprise Server Red Hat Enterprise Linux For more information on the specific versions and additions, visit Dell.com/OSsupport .	
Rack support	ReadyRails™ II sliding rails for tool-less mounting in 4-post racks with square or unthreaded round holes or tooled mounting in 4-post threaded hole racks, with support for optional tool-less cable management arm.	
OEM-ready version available	From bezel to BIOS to packaging, your servers can look and feel as if they were designed and built by you. For more information, visit Dell.com/OEM .	
Recommended support	Dell ProSupport Plus for critical systems or Dell ProSupport for premium hardware and software support for your PowerEdge solution. Consulting and deployment offerings are also available. Contact your Dell representative today for more information. Availability and terms of Dell Services vary by region. For more information, visit Dell.com/ServiceDescriptions .	

Recommended services

ProSupport Plus with SupportAssist provides proactive and predictive support for critical systems. ProSupport provides comprehensive hardware and software support. Get more from your technology starting on day one with ProDeploy Enterprise Suite deployment offers. For more information, visit Dell.com/itlifecycleservices.

End-to-end technology solutions

Reduce IT complexity, lower costs and eliminate inefficiencies by making IT and business solutions work harder for you. You can count on Dell EMC for end-to-end solutions to maximize your performance and uptime. A proven leader in Servers, Storage and Networking, Dell EMC Services deliver innovation at any scale. And if you're looking to preserve cash or increase operational efficiency, Dell Financial Services™ has a wide range of options to make technology acquisition easy and affordable. Contact your Dell Sales Representative for more information.*

Learn more at Dell.com/PowerEdge

* Leasing and financing provided and serviced by Dell Financial Services L.L.C. or its affiliate or designee ("DFS") for qualified customers. Offers may not be available or may vary in certain countries. Where available, offers may be changed without notice and are subject to product availability, credit approval, execution of documentation provided by and acceptable to DFS, and may be subject to minimum transaction size. Offers not available for personal, family or household use.



Dell Precision Rack 7000 Series (7910)

Ultimate performance and security in a 2U Form factor

Why a rack? Because your work demands it.

When the job calls for more security and flexibility in remote or virtualized workstation environments, the Dell Precision Rack 7910 delivers.

- If security is top priority, you need more than a lock and key. Safely house your intellectual property in the datacenter
- Inhospitable or hazardous environment? Need a quiet, cool workspace? Provide employees with workstation-class performance remotely so they can stay productive no matter where they work

Flexible deployment for 1:1 or virtualized 1: many environments – with ISV Certifications

- Deploy 1:1 with optional Dell Wyse 5030/7030 PCoIP Zero Clients for remote connectivity to provide a superb, responsive workstation experience
- For virtualized VMware ESXi and Citrix environments, extend productivity and security benefits to multiple users via 1-4 users with GPU passthrough
- For even greater scalability, deploy Nvidia's Grid technology for one-to-many (shared graphics) virtualized workstation users running true OpenGL 4.X/DX11 based applications

Peak performance and smart design

Experience the same power and scalability as our highest-performing tower workstation, with the convenience of a slim 2U design.

- Take on the toughest most complex applications/workloads including workstation virtualization environments with 1 or 2 Intel® Xeon® Processors (E5-2600 v4) with up to 44 total cores
- Easily manage huge data sets with up to 1TB^{1,2} of 2400MHz DDR4 quad-channel ECC memory
- Powerful in and out-of band systems management with Dell OpenManage™ portfolio featuring Dell Integrated Remote and Lifecycle Access Controller
- New professional grade AMD FirePro™ or NVIDIA® Quadro® graphics plus NVIDIA Grid option

Seamlessly run your software applications

- Dell Precision Optimizer 3.5 auto-tunes application settings for up to 121% application performance improvement
- The result of hundreds of engineering hours and rigorous testing, Independent Software Vendor (ISV) Certifications offer peace of mind that your professional software applications run as designed

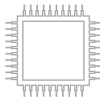
Feature Precision Rack 7000 Series (7910) Technical Specification					
Processor Options	One or two Intel® Xeon® processor E5-2600 v4 Series with up to 22 cores per CPU and Intel Advanced Vector Extensions, Intel Trusted Execution Technology, Intel AES New instructions, Optimized Intel Turbo Boost and optional Intel vPro™ technology				
Operating System Options	Windows® 10 Professional (64 bit) Windows® 8.1 Professional (64-Bit) Windows® 7 Professional (64-Bit)	Red Hat® Enterprise Linux® 7.0 and 7.2 (required for Xeon E5-2600 v4 CPUs RHEL 6.5 supported, future 6.8 for E5-2600 v4)		VMware ESXi 5.5 U2 VMware ESXi 6.0 Citrix XenServer 6.5	
Chipset	Intel® C612				
Memory Options	Quad channel memory up to 1TB 2400MHz DDR4 ECC memory with dual CPUs, 24 DIMM Slots (12 DIMMs per CPU). Note: memory speed is dependent on specific Intel Xeon E5-2600 v4 Series processor installed				
Graphics ⁴ Options	Support for up to 4 PCI Express® x16 Gen 2/Gen 3 graphics cards (2 in x16 slots, 2 in x16/8 slots – requires dual CPUs) Up to 600W graphics (total up to 4 x 150W single width or up to 2 x 300W double width graphics cards				
	High end 3D cards: AMD FirePro W9100 NVIDIA Quadro M6000 NVIDIA Quadro K6000 NVIDIA Quadro M5000 NVIDIA Grid K2a	Mid-range 3D cards: AMD FirePro W5100 NVIDIA Quadro M4000 NVIDIA Quadro K2200 NVIDIA Quadro M2000	Entry 3D cards: NVIDIA Quadro K620 Integrated VGA graphics motherboard connector (part of iDRAC8 Systems Management and requires iDRAC8 Enterprise license to enable)		Professional 2D cards: NVIDIA NVS 510 NVIDIA NVS 310
Storage Options	Support for up to (4) M.2 PCIe SSDs and up to (8) 2.5" SATA/SAS drives . Optional miniPERC PCIe controllers required for SAS				
	M.2 PCIe SSD (NVMe) Up to (4) 1TB drives on Dell Precision Ultra-Speed Drive Quad. PCIe SSD HH/HL card Up to (2) Intel 1.2TB PCIe SSD NVMe drives	2.5" SATA SSD Up to (8) 1TB drives 2.5" SAS SSD Up to (8) 400GB drives	2.5" SATA SSD Up to (8) 1TB drives	2.5" SATA 7200 RPM Up to (8) 1TB 7200 RPM	2.5" SAS 10K RPM 12Gb/s Up to (8) 1.8TB 2.5" SAS 15K RPM 12Gb/s Up to (8) 600GB
Storage Controller	Integrated: 2 x Intel chipset AHCI 6Gb/s SATA controllers with 4 ports (total 8) each for HDD/SSD. One port for optical drive (Supports Intel RSTe software RAID 0, 1,5,10 across 4 ports on 1st controller only. (Maximum 4 drives in RAIDset) Optional: Mini-PERC H330 12Gb/s SAS (6Gb/s SATA) 8 port PCIe controller supports software RAID 0,1,5,10 Mini-PERC H730P PCI-e SAS 12Gb/s (SATA 6Gb/s) PCIe controller with 1GB cache memory and backup - supports hardware RAID 0/1/5/10 on Rack 7910. Note Mini-PERC cards use a Mini-PERC slot and do not consume riser card PCIe slots				
Network Daughter Cards	Base: Intel® i350-Quad port 1Gb Ethernet Network Daughter Card (4 x 1Gb ports), Optional: Intel® X540-Dual port 10Gb + Intel i350 Dual port 1Gb Ethernet Network Daughter card (2 x 10Gb + 2 x 1Gb ports) Intel® X710* Dual port 10Gb DA/SFP+, + i350 Dual port 1Gb Ethernet Network Daughter card Intel® X710* Dual port 10Gb SR/SFP+, + i350 Dual port 1Gb Ethernet Network Daughter card, with SR Optics Intel® X710* Quad Port 10Gb DA/SFP+ Ethernet, Network Daughter Card Intel® X710* Quad Port 10Gb DA/SFP+ Ethernet, Network Daughter Card, with SR Optics Integrated: Integrated Broadcom® BCM5461 Ethernet LAN 10/100/1000 for iDRAC8 controller use with System Management tool suite Optional: Host Bus Adapters: Emulex LPE 12002, Dual Port 8Gb Fibre Channel HBA, QLogic 2562, Dual Port 8Gb Optical Fibre Channel HBA				
1:1 Remote Workstation Access Solutions	Teradici dual and quad display PCoIP™ PCIe remote access host cards & Teradici PCoIP® Workstation Access Software (on host workstation) Dell Wyse 5030/7030 PCoIP Zero clients & Teradici soft clients for Windows and IOS client devices				
Manageability	Dell OpenManage™ portfolio options that include Dell's exclusive Integrated Dell Remote Access Controller (iDRAC) with Lifecycle Controller – includes one VGA graphics connection, Intel® vPro™ Technology's advanced management features (optional, requires Intel WiFi® Link WLAN)				
Optional add-in cards	Optional: Dell Precision Ultra-Speed Drive Duo (HH/HL,x8) & Ultra-Speed Drive Quad (FH/FL,x16) with active cooling. Support for up to 2 and 4 M.2 PCIe NVMe SSDs respectively. Optional 1394 a/b PCIe Card (3 Ports – 2x 1394b + 1x 1394a)			Dual & quad display Teradici PCoIP PCIe remote workstation access cards (for host workstation) Optional Serial Port PCIe Card	
I/O Ports	Front 1 – USB 2.0 1 – USB 2.0 Management port (iDRAC8) 1 - VGA Port for iDRAC8 1 - vFlash Media Slot		Internal 1 – USB 2.0 Dual SD Module connector		Rear 2 – USB 3.0 4 – RJ45 Network 1 - RJ45 for iDRAC8 1 - VGA Port for iDRAC8 1 – Serial
Chassis	HxWxD: 3.41" x 17.0" x 28.37" (29.78" with bezel); 8.66cm x 43.18cm x 72.06cm (75.64cm with bezel) Bays: (1) external slimline optical bay; (8) internal 2.5" bays (support total of (8) 2.5" HDD/SSD drives) Slots: Up to seven PCIe full-length Gen 3 slots (with dual CPUs) in 3 riser cards, maximum 2 double width x16 cards • With single CPU – 3 X x16 (wired as x8) slots (default) or alternative - 1 X x16 & 1 X x16 (wired as x8) slots • With dual CPUs - 1 x16, 3 x16 (wired as x8), 3 low profile x8 (default) or alternative - 2 x16, 1 x16 (wired as x8), 3 low profile x8 Power Supply: One or two redundant hot pluggable 1100W –90% efficient (80PLUS Gold Certified)				
Storage devices	Slimline options: DVD-ROM; DVD+/-RW				
Security Options	Trusted Platform Module (TPM 1.2 or TPM 2.0); Chassis Intrusion switch; Setup/BIOS Password; I/O Interface Security; lockable front bezel; Dell Data Protection (DDP): DDP Security Tools for authentication; DDP Protected Workspace for malware; DDP Encryption for data protection				
Regulatory & Environmental	Energy Star® configurations available including 80 PLUS® registered Gold power supplies; EPEAT® registered (see epeat.net for specific registration rating/status by country); China CECP; GS Mark. For a complete listing of declarations & certifications, see Dell's regulatory & compliance homepage at dell.com/regulatory_compliance				
Warranty & Support Services	3-Year Limited Hardware Warranty and 3-year NBD On-Site Service after Remote Diagnosis Optional: Dell ProSupport is designed to rapidly respond to your business's needs, help protect your investment and sensitive data, and provide enhanced proactive support services to help reduce risk and complexity within your IT environment				
TAA Configurations	Yes				

Some options available only in select regions; ISV certification applies to select configurations 1. A 64-bit operating system is required to support 4GB or more of system memory; 2. GB means 1 billion bytes and TB equals 1 trillion bytes; actual capacity varies with preloaded material and operating environment and will be less; Copyright 2016 Dell Inc. All rights reserved. Intel and Xeon are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States of America and other countries. Microsoft, and Windows are trademarks or registered trademarks of Microsoft Corporation in the U.S. and other countries. . Other trademarks or trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell disclaims proprietary interest in the marks and names of others. Reproduction in any manner whatsoever without express written permission from Dell Inc. is strictly forbidden.



Ultimate performance and security in a 2U Form factor.

PRECISION 7920 RACK



Powerful performance

Power through the most complex, demanding applications more quickly with a new generation of dual-socket performance with the Intel® Xeon® processor Scalable family featuring up to 28 cores per processor. System memory is expandable up to 3TB of faster 2666MHz with select processors (future availability). In addition, every Dell Precision comes with the exclusive Dell Precision Optimizer, which automatically tunes your workstation to run some of the most popular (ISV) applications at the fastest speeds possible.



Latest technology

Ready for complex projects, including virtual reality workflows, with next generation AMD Radeon Pro™ and NVIDIA Quadro® professional graphics with support for up to 900W of graphics power. No project is too big with up to 48TB of total storage featuring Enterprise class SAS hard drives and Dell Precision Ultra-Speed drives with up to 8 M.2 PCIe NVMe SSDs.



Innovative design

Ideal for secure remote users (1:1) the new industrial 2U design fits seamlessly into your datacenter and delivers the same power and scalability as our highest-performing tower workstation. The Integrated Dell Remote Access Controller (iDRAC) allows you to deploy, update, monitor and maintain remote workstations with ease.



Outstanding reliability

Precision Workstations are tested (Independent Software Vendor certified) to ensure the high-performance applications you rely on every day run smoothly. Maintain high-availability with dual redundant and removable power supplies.

Features & Technical Specifications



Feature	Precision 7920 Rack Technical Specifications
Processor Options	One or two Intel® Xeon® processor Scalable family CPUs with up to 28 cores per processor and Intel Advanced Vector Extensions, Intel Trusted Execution Technology, Intel AES New instructions, Optimized Intel Turbo Boost and optional Intel vPro™ technology
Operating System Options	Windows 10 Pro for Workstations (up to 4 Cores) Windows 10 Pro for Workstations (4 Cores Plus) Windows 10 Pro for Workstations Downgrade to Windows 7 (up to 4 Cores) Windows 10 Pro for Workstations Downgrade to Windows 7 (4 Cores Plus) Red Hat® Enterprise Linux® 7.3 Ubuntu Linux 16.04 Suse Linux (SLES 12 SP2) supported NeoKylin 6.0 SP3 (China only)
Chipset	Intel® C621 (Lewisburg)
Memory Options ¹	Six channel memory up to 1.5TB 2666MHz DDR4 ECC memory with dual CPUs, up to 3TB with select CPU SKUs (future availability) 24 DIMM Slots (12 DIMMs per CPU). Note: memory speed is dependent on specific Intel Xeon Processor Scalable processor installed Support for 3 PCI Express® x16 Gen 3 graphics cards ¹ - up to 900W with 3 x 300W double width graphics cards (dual CPU configuration) 1600W PSU recommended for maximum configurations and some restrictions apply
Graphics Options	High end 3D cards: Radeon™ Pro WX 9100 Radeon™ Pro SSG (future) NVIDIA Quadro GP100 NVIDIA Quadro P6000 NVIDIA Quadro P5000 Mid-range 3D cards: Radeon™ Pro WX 7100 Radeon™ Pro WX 5100 NVIDIA Quadro P4000 NVIDIA Quadro P2000 Entry 3D cards: NVIDIA Quadro P600 NVIDIA Quadro P400 Integrated VGA graphics motherboard connector (part of iDRAC9 Systems Management and requires iDRAC9 Enterprise license to enable) Professional 2D cards: NVIDIA NVS 310
Storage Options ²	Support for up to (8) 2.5" or 3.5" SATA/SAS drives, Up to 8 x M.2 NVMe PCIe SSDs via 2 x Dell Ultra-Speed Drive Quad x16 cards (maximum requires dual CPUs), NVMe RAID 0,1,10 option on 1st card (Intel RSTe vROC). PERC PCIe controllers required for SAS drive support M.2 NVMe PCIe SSDs Up to 8* x 1TB drives on 2 Dell Precision Ultra-Speed Drive Quad x16 cards. *Requires dual CPU config. 2.5" SATA SSD Up to 8 x 1TB 2.5" SAS SSD Up to 8 x 800GB 2.5" SATA 7200 RPM Up to 8 x 2TB 3.5" SATA 7200 RPM Up to 8x 8TB (future) 2.5" SAS 10K RPM 12Gb/s Up to 8 x 1.8TB 2.5" SAS 15K RPM 12Gb/s Up to 8 x 600GB

Storage Controller	<p>Integrated: 2 x Intel chipset AHCI 6Gb/s SATA controllers with 4 ports (total 8) each for HDD/SSD. One port for optical drive</p> <p>Intel RSTe software RAID 0, 1,5,10 supported across 4 SATA ports on 1st controller only. (Maximum 4 drives in RAIDset)</p> <p>Intel RSTe (vROC) software RAID 0,1,10 option (motherboard activation key) for M.2 NVMe PCIe SSDs on 1st Dell Ultra-Speed Drive Quad x16 or Duo x8 card (0,1). Customer kit available for Intel RSTe (vROC) motherboard activation key for NVMe RAID support.</p> <p>Optional: PERC H330 12Gb/s SAS (6Gb/s SATA) 8 port PCIe controller supports JBOD and software RAID 0,1,5,10</p> <p>PERC H730P PCI-e SAS 12Gb/s (SATA 6Gb/s) Hardware RAID PCIe controller with 1GB cache (Super Cap backup, RAID 0/1/5/10 (no JBOD)</p> <p>PERC H740P PCI-e SAS 12Gb/s (SATA 6Gb/s) Hardware RAID PCIe controller with 4GB cache (Super Cap backup), RAID 0/1/5/10 (no JBOD)</p> <p>Note: Windows 7 is not supported on the PERC H740P controller. PERC controllers are installed in Slot 3</p>
Network Daughter Cards	<p>Base: Intel® i350-Quad port 1Gb Ethernet Network Daughter Card (4 x 1Gb ports),</p> <p>Optional: Intel® X550-Dual port 10Gb + Intel I350 Dual port 1Gb Ethernet Network Daughter card (2 x 10Gb + 2 x 1Gb ports)</p> <p>Intel® X710* Dual port 10Gb DA/SFP+, + I350 Dual port 1Gb Ethernet Network Daughter card</p> <p>Integrated: Integrated Broadcom® BCM54210 Ethernet LAN 10/100/1000 for iDRAC9 controller use with System Management tool suite</p>
1:1 Remote Workstation Access Solutions	<p>Optional: Teradici Dual and Quad display PColP™ PCIe remote access host cards</p> <p>Wyse 5030/7030 PColP Zero clients. Teradici PColP software clients for Windows, Mac, IOS, Android and ChromeOS available from Teradici</p>
Manageability³	<p>Dell OpenManage™ portfolio options that include Dell's exclusive Integrated Dell Remote Access Controller (iDRAC) with Lifecycle Controller – includes one VGA graphics connection, Intel® vPro™ Technology's advanced management features (optional, requires Intel WiFi® Link WLAN)</p>
Add-in cards	<p>Optional: Dell Precision Ultra-Speed Drive Duo (HH/HL,x8 card) and Ultra-Speed Drive Quad (FH/FL,x16 card) with active cooling.</p> <p>Support for up to 2 and 4 M.2 NVMe PCIe SSDs respectively.</p> <p>USB 3.1 (Gen 2) 10Gb/s Type C card (2 ports) 1 DP pass-through port</p> <p>Optional: Dual & quad (FH card) display Teradici PColP PCIe remote workstation access cards. Full height and low profile bracket versions of dual display card available.</p> <p>Serial Port PCIe Card (single port)</p>
I/O Ports	<p>Front</p> <p>1 – USB 2.0</p> <p>1 – USB 2.0 Management port (iDRAC9)</p> <p>1 - VGA Port for iDRAC9</p> <p>Internal</p> <p>1 – USB 3.1 Type A – supports standard USB storage key</p> <p>SD Vflash media connector</p> <p>Rear</p> <p>2 – USB 3.1 Type A</p> <p>4 – RJ45 Network</p> <p>1 – Serial</p> <p>1 – RJ45 for iDRAC</p> <p>1 – VGA Port for iDRAC</p>
Chassis	<p>HxWxD: 3.41" x 17.0" x 28.37" (29.78" with bezel); 86.8mm x 482mm x 715.5mm (751.3mm with bezel)</p> <p>Bays: (1) external slimline optical bay; (8) front accessible 3.5" bays (support total of (8) 3.5" or 2.5" HDD/SSD drives)</p> <p>Slots: All slots PCIe Gen 3. (6) PCIe full height/full length slots, (1) PCIe full height/half length slot, (1) PCIe low profile/full length slot</p> <p>Up to (3) double width x16 cards supported. All slots x16 mechanically.</p> <ul style="list-style-type: none"> • With single CPU – (1) x x16, (1) x x8, (1) x x8 half length, (1) x x8 low profile PCIe slots • With dual CPUs (2) x x16, (2) x x8 PCIe slots <p>Power Supply: One or two redundant hot pluggable 1100W –90% efficient (80PLUS Gold Certified), Available 1600W PSU is required for certain configurations</p>
Storage devices	<p>Slimline options: DVD-ROM; DVD+/-RW BD-RE</p>

**Security Options
(Check regional
availability)**

Trusted Platform Module (TPM 1.2 or TPM 2.0); chassis Intrusion switch; Setup/BIOS Password; I/O Interface Security; lockable front bezel, Dell Data Guardian, Dell Endpoint Security Suite Enterprise

**Regulatory and
Environmental**

For a complete listing of declarations & certifications, see Dell's regulatory & compliance homepage at dell.com/regulatory_compliance

**Warranty & Support
Services⁴**

3-Year Limited Hardware Warranty and 3-year NBD On-Site Service after Remote Diagnosis
Optional: Dell ProSupport is designed to rapidly respond to your business's needs, help protect your investment and sensitive data, and provide enhanced proactive support services to help reduce risk and complexity within your IT environment

TAA

YES (check regional availability)



ISV certification applies to select configurations:

¹ GB means 1 billion bytes and TB equals 1 trillion bytes; actual capacity varies with preloaded material and operating environment and will be less.

³ Computrace is not a Dell offer. Certain conditions apply. For full details, see terms and conditions at www.absolute.com/en/about/legal/agreements.

⁴ Systems Management Options: Intel® vPro Technology - Fully vPro-capable at point of purchase; the vPro systems management option requires vPro processors. Includes support for Intel Advanced Management Technology (AMT) 9.x. Intel® Standard Manageability - Fully enabled at point of purchase, the Intel Standard Management option is a subset of the AMT features. ISM is not upgradeable to vPro technology post-purchase. No Out-of-Band Systems Management - This option entirely removes Intel out of band systems (OOB) management features. The system can still support in band management. OOB management support through AMT cannot be upgraded post-purchase.

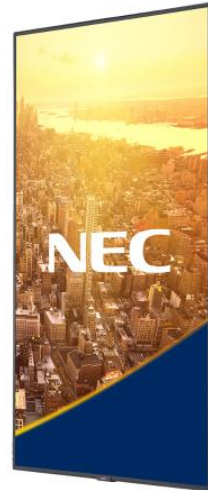
⁵ Availability and terms of Dell Services vary by region. For more information, visit Dell.com/servicecontracts/global; Limited Hardware Warranty available by writing Dell USA LP, Attn: Warranties, One Dell Way, Round Rock, TX 78682 or see www.dell.com/warranty; Onsite Service after Remote Diagnosis: Remote Diagnosis is determination by online/phone technician of cause of issue; may involve customer access to inside of system and multiple or extended sessions. If issue is covered by Limited Hardware Warranty (www.dell.com/warranty) and not resolved remotely, technician and/or part will be dispatched, usually within 1 business day following completion of Remote Diagnosis. Availability varies. Other conditions apply.

Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners. Intel and the Intel logo are trademarks of Intel Corporation in the U.S. and/or other countries. Microsoft and Windows are trademarks of Microsoft Corporation in the U.S. and/or other countries.

MultiSync® C501

LCD 50" Value Large Format Display

Datasheet



Seamless integration for great visual performance

Its thin bezel and super slim design perfectly complements today's modern surroundings whilst multiple display inputs support flexibility and freedom. With fixing points conveniently located on the back of the screen, external equipment can be attached with seamless simplicity. Reasonable brightness levels offer visibility in controlled light surroundings. The professional haze filter is allowing excellent readability. Landscape and portrait capability matches the needs of both corporate huddle spaces and retail signage applications. With a built-in media player, the NEC C Series runs content directly from a USB drive or microSDHC card as a standalone solution but can also download contents via network. Futureproof connectivity handles input from multiple sources. Don't let technology impact design – get seamless integration with the NEC C Series!

Benefits

Impressive FullHD LCD technology – eye-pleasing black levels and impressive contrast ratios for ergonomic viewing and less fatigue in conferencing scenarios.

Modern and slim design – robust yet elegant allowing for an unobtrusive integration into any application and environment.

All-in-one Signage solution integrated – the integrated media player for simple signage use supports easy content playback and management.

Mission-critical 24/7 ready operation – the meticulous selection of industrial-grade components and careful design focused on demanding usage scenarios accompany an impressive and continuous viewer experience.

Ease of use and operation – Smart installation, operation and maintenance functionality ensures accurate performance over the entire lifetime of the display saving time, effort and resources.

Free Download of Multi-Display Management Software – with NaViSet Administrator 2 you can manage all your connected display devices from a centralised location.

Product Information	
Product Name	MultiSync® C501
Product Group	LCD 50" Value Large Format Display
Order Code	60004237

Display	
Panel Technology	AMVA3 with Edge LED backlights
Active Screen Area (W x H) [mm]	1,095 x 616
Screen Size [inch/cm]	50 / 125.7
Brightness [cd/m²]	400, 280 Eco (shipment setting)
Contrast Ratio (typ.)	4000:1
Viewing Angle [°]	178 / 178 (at contrast ratio > 10:1)
Colour Depth [bn]	1.073 (10bit)
Response Time (typ.) [ms]	6.5 (grey-to-grey)
Haze Level [%]	Pro (44)
Supported Orientation	Face Up; Landscape; Portrait

Synchronisation Rate	
Horizontal Frequency [kHz]	31.5 - 91.1 (analog and digital)
Vertical Frequency [Hz]	24 - 85

Resolution	
Native Resolution	1920 x 1080
Supported Resolutions	1920 x 1200; 1920 x 1080; 1680 x 1050; 1600 x 1200; 1440 x 900; 1400 x 1050; 1360 x 768; 1280 x 1024; 1280 x 960; 1280 x 800; 1280 x 768; 1280 x 720; 1024 x 768; 800 x 600

Connectivity	
Input Video Analogue	1 x VGA
Input Video Digital	1 x DisplayPort (with HDCP); 3 x HDMI (with HDCP)
Input Audio Analogue	2 x 3,5 mm jack
Input Audio Digital	1 x DisplayPort; 3 x HDMI
Input Control	1 x LAN 100Mbit; 1 x Remote Control (3.5 mm jack); 1 x RS232
Input Data	1 x microSD (MediaPlayer); 1 x USB 2.0 (MediaPlayer)
Output Audio Analogue	1 x 3,5 mm jack
Output Control	remote control wire (3,5mm jack)

Sensors	
Ambient Light Sensor	Integrated, triggered actions programmable
Temperature Sensor	Integrated, 3 sensors, triggered actions programmable

Electrical	
Power Consumption [W]	65 shipping
Power Savings Mode [W]	< 0.5; < 2 (Networked Standby)
Power Management	VESA DPMS

Environmental Conditions	
Operating Temperature [°C]	+0 to +40
Operating Humidity [%]	20 to 80

Mechanical

Dimensions (W x H x D) [mm]	1,125 x 645 x 45
Weight [kg]	16.1
Bezel Width [mm]	12.4 (left and right); 12.4 (top and bottom)
VESA Mounting [mm]	300 x 300 (FDMI); 4 holes; M6
Ingress Protection	IP5X (front); IP2X (back)

Additional Features

Special Characteristics	Ambient Light Sensor; AMX NetLinX Support; ASCII Control Commands; Automated Email Alert; CEC Support; Crestron Connected Support; Crestron RoomView Support; Display Browser Control; Emergency Notification; Full System Scheduler; KeyGuide; MediaPlayer with Browser Control; NaViSet Administrator 2; OmniColor Control; OSD rotation for portrait mode; PJLink Support; Powered USB-Port; Removable Logo; Secure Mode Operation; Slim LED Indicator; SNMP Support; TileMatrix (10 x 10)
Colour Versions	Black Front Bezel, Black Back Cabinet
Safety and Ergonomics	CE; EMC Class B; FCC; PSB; RoHS; TÜV GS; UL/C-UL or CSA; VCCI
Audio	Integrated Speakers (10 W + 10 W)
Shipping Content	CD-ROM (User Guides/Manuals); Display; Power Cable; Remote Control; VGA cable
Warranty	3 years warranty incl. backlight; additional services available
Operating Hours	24/7

Available Options

Accessories	Feet (ST-401); Trolley (PDMHM-L); Wall mount (PDW C L and P, PD02W T M L, PD03W T M P)
-------------	--

MediaPlayer

Supported Image Formats	JPG (baseline, progressive, RGB, CMYK); max. resolution 5000 x 5000; PNG (interlace, alpha channel); max. resolution 4000 x 4000
Supported Video Formats	MP4 / MOV / FLV (video H.264, audio MP3, AAC); max. resolution 1080p at 30 Hz, 1080i at 60 Hz; MPG (video mpeg1/2, audio mpeg audio layer2/3, AAC-LC); MP @ ML, MP @ HL; WMV (video H.264, wmv advanced L3, wmv simple / main, audio mp3 wmv std); max. resolution 1080p at 30 Hz, 1080i at 60 Hz
Supported Audio Formats	MP3 (MP3); max. bit-rate 320 kBit/s; WAV (LPCM); max. 48 kHz sampling
Supported File Storage / File System	MicroSDHC / FAT16, FAT32; USB 2.0 / FAT16, FAT32

Green Features

Energy Efficiency	Ambient light sensor; Annual energy consumption: 110 kWh (based on 4 operating hours per day); Carbon savings meter; Energy efficiency class: A
Ecological Materials	Manuals on CD; Optional feet
Ecological Standards	EnergyStar 7.0



This document is © 2017 NEC Display Solutions Europe GmbH.

All rights reserved in favour of their respective owners. All hardware and software names are brand names and/or registered trademarks of the respective manufacturers. All specifications are subject to change without notice. Errors and omissions are excepted. 19.12.2017

HP LaserJet Pro 200 color Printer M251 series



Produce professional colour documents that help boost business. Print from virtually anywhere with HP ePrint¹. Use business apps to access and print from the web^{2,3}. Locate the printer anywhere in the office, using wireless connectivity^{3,4}.



Highlights

- First page out in as fast as 18.5 secs
- Print speed of up to 14 ppm black & colour
- 128 MB RAM
- 1 Hi-Speed USB 2.0 port; 1 Ethernet and 1 USB port
- Recommended monthly page volume: 250 – 1,500



Ethernet



Colour touchscreen



Wireless



ePrint



Auto on/Auto off



Color printing
up to 14ppm

Enjoy fast set up and easy, web-connected printing.

- Use business apps and the 8.9 cm (3.5-in) colour touchscreen to access and print from the web^{2,3}.
- Use the colour touchscreen to preview and select the pictures that you want to print from your flash drive³.
- Install your printer fast – there's no CD required with HP Smart Install⁵.
- Print directly from a flash drive using the easy-access USB port³.

Maintain the pace of business with mobile printing.

- Print from virtually anywhere with HP ePrint¹.
- Print wirelessly from your iPad®, iPhone®, and iPod touch® with AirPrint™⁶.
- Send files from a mobile device directly to your printer – without a network – using HP wireless direct printing^{3,7}.
- Set up and share the printer anywhere in the office with wireless and built-in Ethernet connectivity^{3,4}.

Create high-impact, colour marketing materials.

- Get accurate colour with HP ImageREt 3600 and ColorSphere II toner. Optimise settings with HP EasyColor.
- Boost productivity with print speeds of up to 14 ppm⁸. Reload the paper tray less often, thanks to the 150-sheet capacity.
- Create impressive colour marketing materials on a range of media, including HP specialty papers.
- Print affordably – get the same black cost per page as a black-only HP LaserJet printer⁹. Save money with the high-capacity HP LaserJet 131X Black Toner Cartridge¹⁰.

Reduce your environmental impact.

- Reduce energy use with HP Auto-On/Auto-Off Technology which turns your printer on when you need it and off when you don't¹¹.
- Save energy and time with Instant-on Technology¹² – start printing and get the first page out as fast as 19 seconds⁸.
- Receive consistent results with Original HP LaserJet toner cartridges and reorder with HP SureSupply¹³.
- Get free, easy recycling: toner cartridges returned through HP Planet Partners are recycled responsibly¹⁴.

HP LaserJet Pro 200 color Printer M251 series

Technical specifications

Print speed	Up to 14 ppm ISO black (A4); Up to 14 ppm ISO colour (A4) Measured using ISO/IEC 24734, excludes first set of test documents. For more information see http://www.hp.com/go/printerclaims . Exact speed varies depending on the system configuration, software application, driver, and document complexity. First page out: As fast as 18.5 sec black (A4); As fast as 19 sec colour (A4)
Print resolution	Up to 600 x 600 dpi black; Up to 600 x 600 dpi colour
Print technology	Laser
Print Area	Print margins: Top: 4.3 mm; Bottom: 4.3 mm; Left: 4.3 mm; Right: 4.3 mm; Maximum print area
Print languages	HP PCL 6, HP PCL 5c, HP Postscript Level 3 emulation (via Universal Print Driver)
Print cartridges number	4 (1 each black, cyan, magenta, yellow)
Mobile printing capability	CF146A: HP ePrint, Apple AirPrint™, Mopria-certified; CF147A: HP ePrint, Wireless direct printing, Apple AirPrint™, Mopria-certified;
Monthly duty cycle	Up to 30,000 pages (A4); Recommended monthly page volume: 250 to 1500
Automatic paper sensor	No
Processor speed	750 MHz
Wireless	CF146A: No; CF147A: Yes, built-in WiFi 802.11 b/g/n, secure wireless direct printing;
Network ready	CF146A: Standard (built-in Ethernet); CF147A: Standard (built-in Ethernet, WiFi 802.11 b/g/n);
Memory	Standard: 128 MB; Maximum 128 MB
Memory card compatibility	None
Hard Disk	None
Media types	Paper (bond, brochure, coloured, glossy, heavy, letterhead, light, photo, plain, preprinted, prepunched, recycled, rough), transparencies, labels, envelopes, cardstock
Media sizes	Supported A4, A5, A6, B5 (JIS); 10 x 15 cm, postcards (JIS single, JIS double); envelopes (DL, C5, B5); Custom: 76 x 127 to 216 x 356 mm
Media Handling	Input capacity: Up to 150 sheets; Up to 10 envelopes envelopes Output capacity: Up to 125 sheets, Up to 10 envelopes Maximum: Up to 125 sheets Duplex printing: Manual (driver support provided)
Paper weight	Supported, by paper path: 60 to 163 g/m² (up to 220 g/m² with HP laser glossy photo papers)
Compatible operating systems	Full software installs supported on: Microsoft® Windows®7 32-bit and 64-bit, Windows Vista® 32-bit and 64-bit, Windows® XP 32-bit (SP2 or higher); Driver only installs supported on: Microsoft® Windows® Server 2008 32-bit and 64-bit, Windows® Server 2003 32-bit (SP3 or higher); Mac OS X v10.5, v10.6, v10.7; Linpus Linux (9.4, 9.5), RED HAT Enterprise Linux 5.0 (supported with a pre-built package); SUSE Linux (10.3, 11.0, 11, 11.1, 11.2), Fedora™ (9, 9.0, 10, 10.0, 11.0, 11, 12, 12.0), Ubuntu® (8.04, 8.04.1, 8.04.2, 8.10, 9.04, 9.10, 10.04), Debian (5.0, 5.0.1, 5.0.2, 5.0.3) (supported by the automatic installer); HP/UX 11 and Solaris® 8/9
Minimum system requirements	Windows: Windows 8, Windows 7, Windows Vista: 1 GHz (32-bit) (x86) or (64-bit) (x64) processor, 1 GB RAM (32-bit) or 2 GB RAM (64-bit), 200 MB free hard disk space, CD/DVD-ROM or Internet, USB or Network port; Windows XP (32-bit) (SP2); Pentium® 233 MHz processor, 512 MB RAM (32-bit) or 2 GB RAM (64-bit), 200 MB free hard disk space, CD/DVD-ROM or Internet, USB or network port Mac: Mac OS X v10.5, v10.6, v10.7; PowerPC G4, G5, or Intel® Core™ Processor; 256 MB RAM; 300 MB free hard disk space; CD/DVD-ROM or Internet; USB or Network port
Duplex printing	Manual (driver support provided)

What's in the box	CF146A: HP LaserJet Pro 200 color M251n printer; Preinstalled introductory HP Black, Cyan, Yellow, Magenta LaserJet Toner Cartridges (~700 pages); CDs containing device software and electronic documentation; Install Guide, Support flyer, Warranty guide; Power cord; CF147A: HP LaserJet Pro 200 color M251nw printer; Preinstalled introductory HP Black, Cyan, Yellow, Magenta LaserJet Toner Cartridges (~700 pages); CDs containing device software and electronic documentation; Install Guide, Support flyer, Warranty guide; Power cord; USB cable;
Supplies	CF210A HP 131A Black Original LaserJet Toner Cartridge 1,600 pages CF210X HP 131X High Yield Black Original LaserJet Toner Cartridge 2,400 pages CF211A HP 131A Cyan Original LaserJet Toner Cartridge 1,800 pages CF212A HP 131A Yellow Original LaserJet Toner Cartridge 1,800 pages CF213A HP 131A Magenta Original LaserJet Toner Cartridge 1,800 pages
Software included	Windows®: HP Installer/Uninstaller, HP PCL 6 print driver, Status Alerts, HP Update, DXP; Mac: HP Installer/Uninstaller, HP Postscript driver, HP Setup Assistant, HP Utility, HP Alerts, HP Firmware Updater
Printer management	Windows®: HP Device Toolbox (default install), SNP Alerts (minimum network install), HP Web Jetadmin (download); Mac: HP Utility
Printer dimensions (W x D x H)	CF146A: 405 x 453 x 250 mm; Maximum 405 x 512 x 250 mm (input tray extended to legal-size) CF147A: 405 x 453 x 265 mm; Maximum 405 x 512 x 354 mm (input tray extended to legal-size, touchscreen control panel rotated up)
Package dimensions (W x D x H)	CF146A: 500 x 333 x 550 mm;
Printer Weight	CF146A: 18.7 kg; CF147A: 18.8 kg;
Package weight	CF146A: 22.77 kg;
Operating environment	Temperature: 15 to 32.5°C, Humidity: 20 to 70% RH
Storage	Temperature: -20 to 40°C, Humidity: 10 to 95% RH
Acoustics	Acoustic power emissions: 6.1 B(A); Acoustic pressure emissions: 47 dB(A)
Power	Requirements: Input voltage: 220 to 240 VAC (+/- 10%), 50 Hz (+/- 3 Hz) Consumption: 315 watts (printing), 11.5 watts (ready), 5.1 watts (sleep), 0.2 watts (off). Typical Electricity Consumption (TEC): 1.222 kWh/Week Internal
Certifications	CISPR 22:2005 +A1 (Class B); EN 55022:2006 +A1 (Class B); EN 61000-3-2 :2006 +A1:2009 +A2:2009; EN 61000-3-3 :2008; EN 55024:1998 +A1 +A2; FCC Title 47 CFR, EMC Directive 2004/108/EC with CE Marking (Europe); other EMC approvals as required by individual countries Energy Star Qualified: Yes
Country of origin	Made in China
Warranty	One-year limited warranty. Warranty and support options vary by product, country and local legal requirements.
Service and support	UM137E - HP 3 Year Care Pack w/Standard Exchange for Color LaserJet Printers (Available in all Europe, Middle East, Africa countries) UM133E - HP 3 Year Care Pack w/Next Day Exchange for Color LaserJet Printers (Available in Austria, Belgium, Denmark, Finland, France, Germany, Ireland, Italy, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, UK, Czech Republic, Greece, Hungary, Poland, Slovakia)

Footnotes

¹ Requires an Internet connection to the printer. Feature works with any connected Internet- and email-capable device. Requires HP Web Services Account Registration. Print times may vary. For a list of supported documents and image types, see www.hp.com/go/eprintcenter. And for additional solutions, see www.hp.com/go/mobile-printing-solutions.; ² Requires a wireless access point and an Internet connection to the printer. Services may require registration. App availability varies by country, language, and agreements. For details, see www.hp.com/go/eprintcenter.; ³ Feature only available on the HP LaserJet Pro 200 Color M251nw Printer.; ⁴ Wireless performance is dependent upon physical environment and distance from access point, and may be limited during active VPN connections.; ⁵ HP Smart Install works with Microsoft® Windows only.; ⁶ Supports the following devices running iOS 4.2 or later: iPad®, iPad® 2, iPhone® (3GS or later), iPod touch® (3rd generation or later). Works with HP's AirPrint-enabled printers and requires the printer be connected to the same network as your iOS device. Wireless performance is dependent upon physical environment and distance from the access point. AirPrint, the AirPrint Logo, iPad, iPhone, and iPod touch are trademarks of Apple® Inc., registered in the U.S. and other countries.; ⁷ Mobile device must be wireless-enabled and within wireless range of the printer. Printer must be HP ePrint-enabled and may require a firmware upgrade. Feature may require the download of drivers or apps to mobile device, available at www.hp.com/go/eprintcenter.; ⁸ Printing speed measured using ISO/IEC 24734 and excludes first set of test documents. For more information, see www.hp.com/go/printerclaims. Exact speed varies depending on the system configuration, software application, driver, and document complexity. FPO exact speed varies depending on the system configuration, software programme, document complexity, network, media width, media weight, environment, and job size.; ⁹ Compared with HP LaserJet Pro P1606dn printer. Assuming customer is printing at least 30% of total pages in colour with content similar to the colour ISO/IEC 19798 test suite (www.iso.org/itc1/sc28) and overall average job length of three pages. Yields established using ISO/IEC test standards. Actual yields and costs vary considerably depending on images printed, number of colour pages printed, and other factors.; ¹⁰ HP 131X LaserJet Black Toner Cartridge not included; please purchase separately.; ¹¹ HP Auto-On/Auto-Off capabilities subject to printer and settings.; ¹² Compared with products that use traditional fusing.; ¹³ Programme features and availability may vary by country. For more information, visit www.hp.com/learn/suresupply.; ¹⁴ Programme availability varies. HP print cartridge return and recycling is currently available in more than 50 countries and territories around the world through the HP Planet Partners programme. For more information, or to request return envelopes and bulk collection boxes, visit www.hp.com/recycle.



<http://www.hp.com/uk>

The product could differ from the images shown. © Copyright 2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

4AA4-2276EEE, October 2014



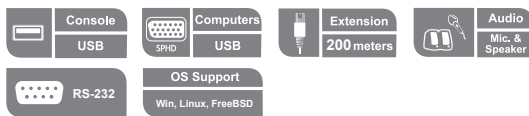
CE750A

USB KVM Extender

The CE750A is a USB-based KVM Extender with automatic signal compensation and RS-232 serial functionality that allows access to a computer system from a remote USB console (USB keyboard, monitor, and USB mouse).

Because it allows access to a computer system from a remote console, the CE750A is perfect for use in any type of installation where you need to place the console where it is conveniently accessible, but you want the system equipment to reside in a safe location – for example away from the dust and dirt of the factory floor or the harsh environment of a construction site.

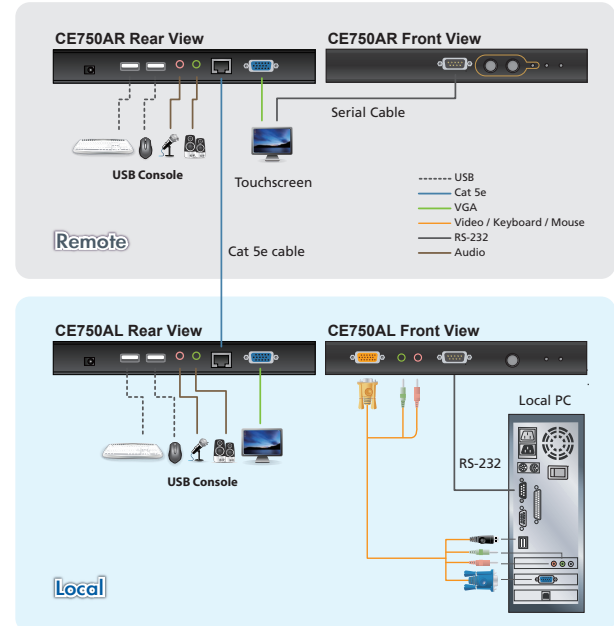
The CE750A improves on previous designs by the addition of an RS-232 port, on both the Local and Remote Units, that allows you to connect to a serial terminal for configuration (Local Unit) or serial devices such as touchscreens and barcode scanners (Remote Unit).



Features

- Local and Remote units connect at distances up to 200 meters using Cat 5e cable
- Dual console operation – control your system from both the local and remote USB keyboard, monitor, and mouse consoles
- Built-in ASIC for greater reliability and compatibility
- USB keyboard and USB mouse ports
- RS-232 serial ports – allows you to connect to a serial terminal for configuration (Local Unit) or serial devices such as touchscreens and barcode scanners (Remote Unit)
- Supports stereo speakers and stereo microphone
- USB overcurrent detection and prevention
- Pushbutton operating mode selection (Local Unit only) – select between Local and Auto operating modes
- Built-in 8KV/15KV ESD protection (contact voltage 8KV, air voltage 15KV) and 2KV surge protection
- Adjustable gain control – automatically and manually adjusts signal strength to compensate for distance
- High resolution video – up to 1920x1200@60Hz at 30m, 1600x1200@60Hz at 150m, 1280x1024@60Hz at 200m
- Supports VGA, SVGA, SXGA (1280 x 1024), UXGA (1600 x 1200), and multisync monitors; local monitor supports DDC, DDC2, DDC2B
- Hot pluggable
- Rack mountable
- Easy to install – no software required, simply connect cables to the devices
- Supports wide screen formats*

* The EDID data for a widescreen is sent from the local video output port. For widescreen modes and displays, connect the monitor to the local video output port or use an ATEN EDID emulator.



Specifications

Function	CE750AL	CE750AR
Connectors		
Console Ports	2 x USB Type A Female (White)	2 x USB Type A Female (White)
	1 x HDB-15 Female (Blue)	1 x HDB-15 Female (Blue)
	1 x Mini Stereo Jack Female (Green)	1 x Mini Stereo Jack Female (Green)
	1 x Mini Stereo Jack Female (Pink)	1 x Mini Stereo Jack Female (Pink)
	1 x DB-9 Female (Black)	1 x DB-9 Male (Black)
	1 x RJ-45 Female	1 x RJ-45 Female
KVM Ports	1 x DC Jack	1 x DC Jack
	1 x SPHD-15 Female (Yellow)	N/A
	1 x Mini Stereo Jack Female (Green)	N/A
LEDs		
Local	1 (Green)	N/A
Remote	1 (Green)	1 (Green)
Link	N/A	1 (Green)
Picture Compensation	N/A	1 (Orange)
Pushbuttons		
Operating Mode Selection	1 x Pushbutton	N/A
Picture Compensation	N/A	2 x Pushbuttons
Emulation		
Keyboard / Mouse	USB	USB
Video	1920 x 1200 @ 60 Hz at 30 m;	1920 x 1200 @ 60 Hz at 30 m;
	1600 x 1200 @ 60 Hz at 150 m;	1600 x 1200 @ 60 Hz at 150 m;
	1280 x 1024 @ 60 Hz at 200 m	1280 x 1024 @ 60 Hz at 200 m
Power Consumption	DC 5.3 V / 2.68 W	DC 5.3 V / 3.6 W
Environmental		
Operating Temperature	0° - 50° C	0° - 50° C
Storage Temperature	-20° - 60° C	-20° - 60° C
Humidity	0 - 80% RH, Non-condensing	0 - 80% RH, Non-condensing
Physical Properties		
Housing	Metal	Metal
Weight	0.47 kg	0.47 kg
Dimensions (L x W x H)	20.20 x 8.01 x 2.50 cm	20.20 x 8.63 x 2.50 cm

ATEN International Co., Ltd.

3F., No.125, Sec. 2, Datong Rd., Sijhih District., New Taipei City 221, Taiwan
Phone: 886-2-8692-6789 Fax: 886-2-8692-6767
www.aten.com E-mail: marketing@aten.com

Publish Date: 06/2016 V1.0



© Copyright 2016 ATEN® International Co., Ltd.
ATEN and the ATEN logo are trademarks of ATEN International Co., Ltd.
All rights reserved. All other trademarks are the property of their respective owners.



Dell 1U Rackmount LED Console

Manage your servers while saving valuable rack space

Dell continues its commitment to large enterprise customers by offering the infrastructure and accessories you need to complement your server installation. A keyboard, monitor, and mouse (KMM) rack console offers IT managers the ability to install a single, integrated user console.

The Dell™ 1U rackmount LED console (model number: FPM185) provides a system administrator's control station mounted directly into a rack enclosure in a slim 1U (1.75-inch) form factor. Combined with an 18.5-inch flat-panel LED screen and a specially designed keyboard and touchpad mouse, this KMM can be mounted in the same rack U-location with any currently shipping Dell KVM (keyboard, video, and mouse) console switch to manage the setup, administration, and maintenance of multiple rackmounted servers.

Ease of installation

The KMM console fits easily into the Dell PowerEdge™ xx20 family of racks, as well as the previous generation PowerEdge 2410 and 4210 racks and third-party racks that meet the EIA-310-E specification. Compatibility with the 1U rackmount sliding rail kit enables quick installation in a rack. The console rail kit uses the ReadyRails™ II interface for tool-less installation in Dell or third-party racks with unthreaded round holes or square holes.

The KMM console supports multiple enterprise configurations. It can be connected directly to the keyboard, video, and mouse ports of a single rackmounted server for a simple one-to-one interface, or it can be attached to a rackmounted Dell KVM console switch, such as the Dell PowerEdge 4322DS, which supports up to 32 servers. A KVM console switch maintains the electrical connection to each server as the KMM rack console is switched by the KVM among the connected systems. The KMM console can also share its 1U space with any of the currently shipping Dell KVMs.

Better for the environment

The Dell 1U rackmount LED console uses an LED-backlit display and is eco-friendly. Unlike the typical LCD console that uses a display backlit by CCFLs (common cathode florescent lamps), the LED console is free of mercury vapor. The console is also RoHS compliant.

Regional support

Dell provides user accessibility for multiple geographic regions. The KMM console can be configured for multiple keyboard options and jumper cords to meet regional needs. Keyboard language options include English (both US International and UK versions), French, Spanish, German, Chinese (Simplified and Traditional), Korean, and Japanese. The keyboard and mouse touchpad are connected to the server or KVM through a cable with a USB interface.

The IEC C13 to C14 jumper cord is pre-installed on the unit and allows for connection to current and legacy power distribution units (PDUs). NEMA and INMETRO cords are also supported for some regions. If an alternate cord is required, the IEC cord can be easily replaced with an alternate jumper cord with a female C13 connector or extended by attaching another cord to the C14 connector.

Key differentiators

The FPM185 has two USB 3.0 compliant pass-through ports, which provide faster data transmission between the KMM and connected USB devices. The 18.5-inch widescreen display supports both legacy server video modes and widescreen video modes. The FPM185 rail kit enables tool-less installation for a typical deployment completed within minutes. The touchpad mouse has palm rejection technology that allows users to rest their palms on the touchpad without causing cursor jumps or page skips.

Features

The 1U KMM rack console provides tool-less rack installation, regional keyboards to support multiple languages, and an LED-backlit widescreen 16:9 monitor. The interface for the keyboard with touchpad mouse provides ease-of-use through a single USB connection.

FPM185		Technical specifications	
Height (rack units)	1U		
Shipping package dimensions (width x depth x height)	29.5" x 8.5" x 23"		
Minimum EIA flange sharing depth (for sharing 1U rack space with Dell KVM)	27.76" (705.1 mm)		
Rail adjustability range without KVM	Square hole rack:	604 mm – 900 mm	
	Round hole rack:	590 mm – 893 mm	
	Threaded hole rack:	604 mm – 914 mm	
Rail adjustability range with KVM	Square hole rack:	705 mm – 900 mm	
	Round hole rack:	691 mm – 893 mm	
	Threaded hole rack:	705 mm – 914 mm	
18.5-inch LED monitor			
Maximum power usage	Less than 20W		
Display type	18.5" LED-backlit a-Si TT LCD module		
Flat panel technology	1366 x 768 WXGA screen with VGA connection		
Diagonal viewable image (height x width)	409.8 mm x 230.4 mm		
Display active area	470.1 mm		
Pixel pitch	300 (per one triad) x 300		
Monitor physical size (width x depth x height)	430.4 mm x 9.9 mm x 254.6 mm		
Weight (LED panel only)	1.29 kg		
Auto-ranging power supply	Input: 110 – 240 V~		
Input device			
Input device	Integrated keyboard and touchpad		
Touchpad	Integrated 80 mm x 45 mm touchpad with palm rejection technology		
Mouse buttons	2 mouse buttons		
Input device interfaces	USB connector for both keyboard and touchpad		
Rail interface			
ReadyRails™ II	Tool-less mounting for square-hole and unthreaded round-hole racks and tooled mounting for threaded round-hole racks		
Ordering configurations			
Ordered as rack accessory	When KMM sold with a Dell rack		
Ordered as KVM accessory	When KMM sold with a Dell KVM		
Ordered as KMM customer kit	When KMM sold as a stand-alone kit		
Ordered as KVM accessory + KVM brackets	When KMM sold with a Dell KVM with the intent to deploy both KMM and KVM in the same 1U of the rack		
Order standalone KVM brackets kit	When the customer has the KMM and Dell KVM and wants to install the KMM/KVM in the same 1U of the rack		

Global services and support

Dell Services can help reduce IT complexity, lower costs, and eliminate inefficiencies by making IT and business solutions work harder for you. The Dell Services team takes a holistic view of your needs and designs solutions for your environment and business objectives while leveraging proven delivery methods, local talent, and in-depth domain knowledge for the lowest total cost of ownership.

Learn more at Dell.com/PowerEdge/Rack

© 2013 Dell Inc. All rights reserved. Dell, the DELL logo, the DELL badge, PowerEdge, and ReadyRails are trademarks of Dell Inc. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell disclaims proprietary interest in the marks and names of others. This document is for informational purposes only. Dell reserves the right to make changes without further notice to any products herein. The content provided is as is and without express or implied warranties of any kind.



DELL DAV2216-G01 KVM switch (A7485896)

16 x KVM, 8 x USB, silver



Now, for your Dell Analog KVM Switch DAV2108 and DAV2116, Dell offers a low cost USB and PS2 Integrated Access Cable provides basic USB and PS2 with VGA connections to your servers with a molded 10ft CAT5 cable to the Dell Analog KVM switch. These are perfect for the server room where the best value for basic performance is expected. Now, you don't have to pay for Virtual Media or Common Access Card support if you don't want it with your Dell Analog Server Console Switch. DUSBIAC-10 provides a low cost USB connection and DPS2IAC-10 is a great alternative to manage legacy PS2 servers on your Dell Analog KVM Switch.

ReadyRails static rails for toolless 1U mounting in 4-post racks with square or unthreaded round holes or tooled mounting in 4-post threaded and 2-post (Telco) racks. Mount this Dell KVM in the same U space with your Dell KMM (DKMMLED185) by adding PN DRMK-77 / A7485911. This is the exclusive 1U mounting bracket for the Dell DMPU and DAV KVM products. Standard Three-Year Warranty (requires registration within 90 days) - 8/5 coverage of your hardware, 10- to 14-day RMA post receipt of failed unit.

- Add a digital channel via a physical hardware key;
- 2 local users;
- Local console USB;
- Widescreen support;
- Hi-res to 1600×1200 (standard) and 1680×1050;
- ACI support for cascading up to 256 servers.

Overview

The Dell Analog KVM switches, engineered by Avocent, are ideally suited for environments where remote access is not required but maximum security is essential. The Analog Server Console Switch is an excellent choice where real-time video and mouse response are required. Its responsiveness is not impacted by the need to digitize and transmit video frames, mouse and keystroke events. For high resolution requirements of a Network Operation Center, the Server Console switches can support resolutions of up to 1600×1200 and widescreen resolutions of up to 1680×1050.

The Analog KVM Server Console Switches provide flexibility to customers who may want to implement remote access in the future, but who are not ready to make that commitment at the time of purchase. The digital capabilities of the Server Console Switch are 'unlocked' by plugging the Dell Remote Access Key into any one of the USB ports of the rear of the switch. With the Dell Remote Access Key installed, one authenticated digital user can remotely manage any one of the servers connected to the Server Console Switch over a TCP/IP network with support for DES, 3DES, AES or 128-bit SSL encryption of both KVM and Virtual Media sessions over a single IP address.

Main specifications:

Networking

Ethernet LAN: Y

Ports & interfaces

Keyboard port type: USB

Mouse port type: USB

Video port type:	VGA
USB 2.0 ports quantity:	8
Ethernet LAN (RJ-45) ports:	16
VGA (D-Sub) ports quantity:	2
USB connector type:	USB Type-A
Video	
Maximum resolution:	1600 x 1200 pixels
Design	
Rack mounting:	1U
Colour of product:	Silver
LED indicators:	Y
Display	
Built-in display:	N
Performance	
Security algorithms:	3DES,AES,DES

*PLEASE NOTE: Every effort has been made to ensure the accuracy of all information contained herein. Lasystems makes no warranty expressed or implied with respect to accuracy of the information, including price, editorials or specifications. Lasystems or its suppliers shall not be liable for incidental, consequential or special damages arising from, or as a result of, any electronic transmission or the accuracy of the information contained herein, even if Lasystems has been advised of the possibility of such damages. Product and manufacturer names are used only for the purpose of identification.

Rittal – The System.

Faster – better – everywhere.

► Technical System Catalogue CMC III Monitoring System



ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

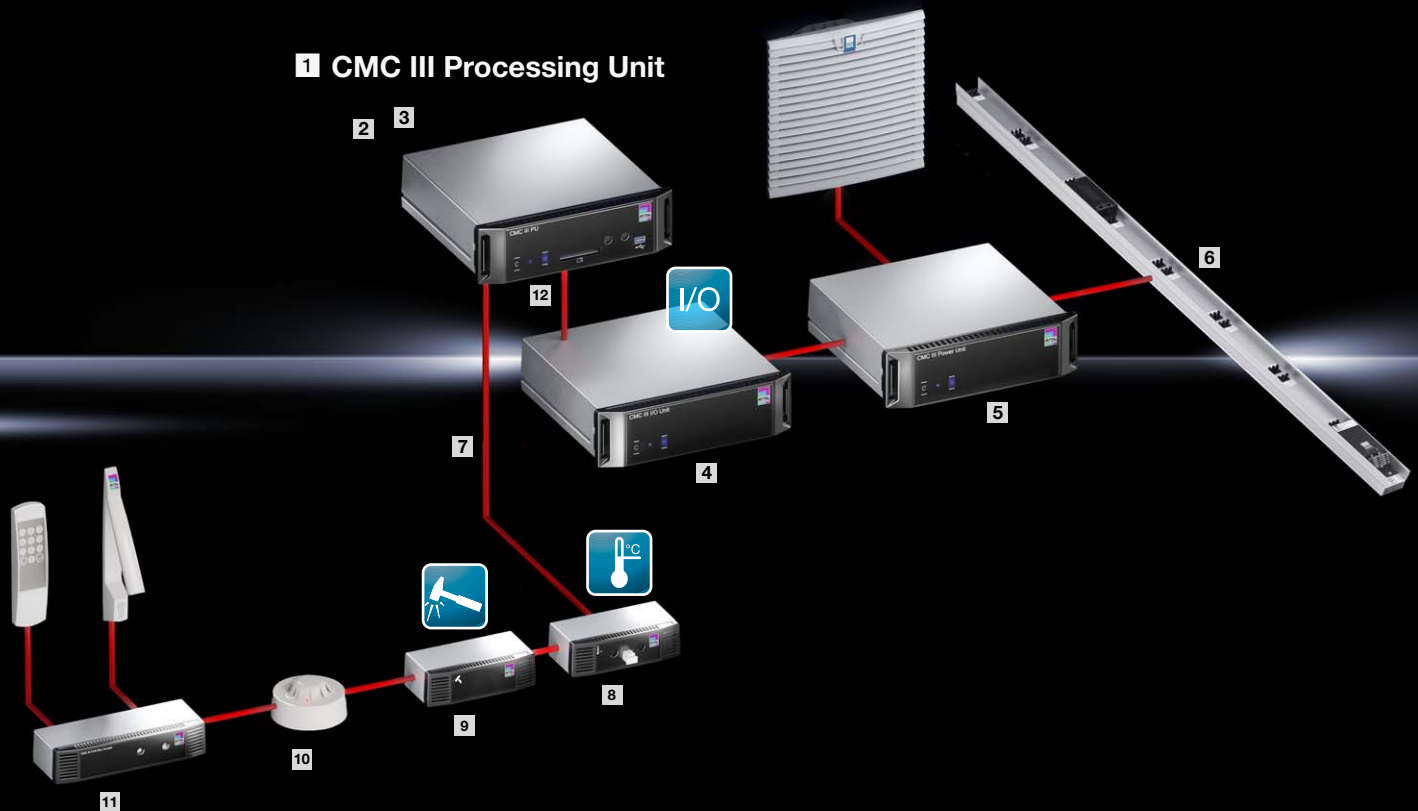
IT INFRASTRUCTURE

SOFTWARE & SERVICES

FRIEDHELM LOH GROUP



CMC III monitoring system



Computer Multi Control (CMC) is an alarm system for network and server enclosures, standard enclosures, containers and rooms.

- It monitors temperatures, humidity, access, fumes, energy and many other physical ambient parameters.
- The system is modular and can be flexibly adapted to meet specific monitoring requirements.

- User benefits plus exceptional savings are achieved thanks to monitoring via the network and the automation of security processes.

Further information can be found at:
www.rittal.com

1 CMC III Processing Unit

2 Power supply

3 Redundant power supply

4 CMC III I/O unit

5 CMC III Power Unit

6 CMC III PSM measuring bar for direct connection

7 Up to 16 CAN bus systems can be connected

8 CMC III temperature sensor

9 CMC III vandalism sensor

10 CMC III smoke alarm

11 CMC III CAN bus access

12 Up to 16 CAN bus systems can be connected

CMC III monitoring system

CMC III monitoring system

The CMC III is an intelligent monitoring system that uses sensors to measure various environmental values. If defined minimum or maximum limit values are breached, alarm notifications can be sent out via e-mail, text message or SNMP.

Thanks to intelligent control mechanisms, outputs can also be switched automatically and access to an enclosure can be controlled and monitored.

Due to its flexible assembly, the system is suitable for a wide range of applications – from minor roles in standalone enclosures to complex requirements for a suite of enclosures.

The benefits of CMC III at a glance:

- Custom selection and placement of sensors
- Minimal cabling work thanks to bus topology
- Sensors connected to a central processing unit through secure CAN bus technology
- Simple installation and rapid start-up thanks to plug-and-play concept
- Automatic sensor detection
- Network-based access using a standard web browser
- Control and programming software already integrated
- Redundant power supply and power over Ethernet (PoE) possible
- Can be incorporated into higher management systems via SNMP, OPC-UA or Modbus/TCP

Operating the CMC III

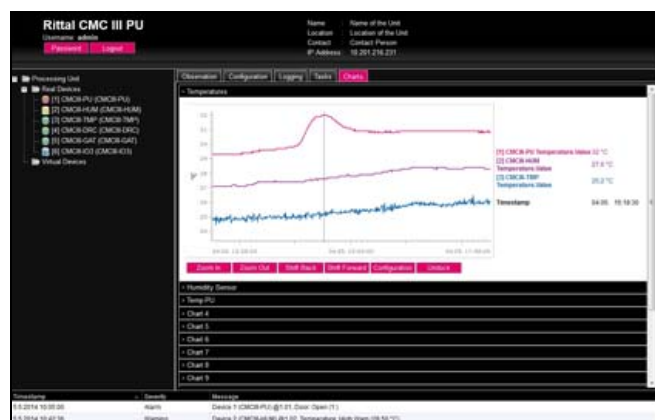
Each CMC III Processing Unit comes with its own integrated website (webserver) as standard. This website can be accessed via the network using just a standard web browser, with no need for additional software or plug-ins.

Access to the functions and measured values of the CMC III is password-protected, and users must have an account on the system and their own password. Alternatively, the CMC III can be connected via LDAP or Radius to an active directory so that user administration can be carried out centrally. The administrator can also use group assignment to manage the rights of users and give them specific write and read rights for each sensor.

The website itself has been kept very simple so that users can get to grips with it quickly, which means that even users with no programming skills can set up and manage the system. The method of operation is based on familiar structures from desktop PCs and alarm scenarios can even be programmed on the website using click commands. A custom view can be designed for day-to-day usage that is activated directly on login. This view allows users both to operate predefined elements of the CMC III interface and create custom lists of variables.

Graphics for sensors and measured values make it easier to operate the system and help users quickly build up an overview. The CMC III can be used to save measured values to an SD card or a USB flash drive and display the values in a graphic on the website. This helps to identify hot spots in the rack and reveal potential opportunities to boost efficiency.

Access to the website can also be managed via https to ensure data is transferred securely in the network. In this case, the connection between the PC and CMC III is encrypted using SSL and access without an encrypted connection from the CMC is no longer supported. Every action that a user executes is also logged by the system. As a result, it is possible to trace exactly which users have made changes to the system so that possible causes can be narrowed down more quickly in the event of an alarm.



CMC III monitoring system

CMC III Processing Unit / Compact

The CMC III Processing Unit and the CMC III Processing Unit Compact are the heart of a CMC III system. This is where all measured values are summarised, evaluated and forwarded.

A CMC III Processing Unit / Compact is the interface between a CMC III system and the user. It is incorporated into the company network and utilises an integrated website to make current values available to every authorised user.

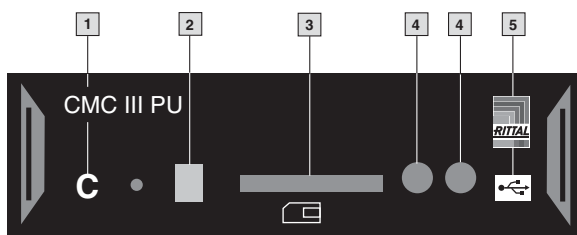
A CMC III Processing Unit / Compact can be powered both in a redundant system via two power packs and using PoE delivered via the connected network cable. The system can be fitted very easily and quickly in the enclosure and incorporates a mounting unit for the enclosure frame and a 1 U mounting unit for up to three devices that can be installed in the 19" section in the enclosure.

Each CMC III Processing Unit / Compact has four sensors already integrated as standard. Besides a socket for the temperature sensor included in the scope of supply, there is also an infrared sensor at the front for monitoring a door and there are two digital inputs at the rear that can, for example, be used to monitor relays.

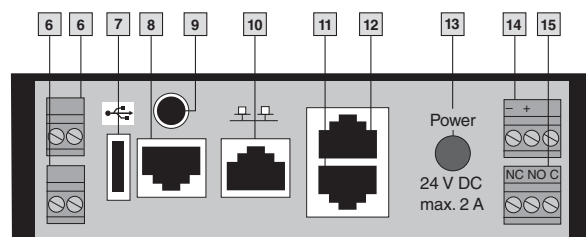
Thanks to the simple and self-explanatory web interface, the system as a whole is intuitive to operate and configure. Users do not need to have a great deal of programming know-how to start-up and manage an entire CMC III system. All that is required is a PC with a standard web browser. The CMC III Processing Unit / Compact represents the state of the art and has the most important network protocols already integrated into it. The new system supports TCP/IPV6 and the secure SNMPv3 protocol.



Connection information



- 1 "C" button for acknowledging notifications
- 2 Multi-LED for the status display
- 3 SD card slot (only on CMC III Processing Unit)
- 4 Integrated infrared access sensor
- 5 Mini USB port for configuration
- 6 Digital inputs (x 2)
- 7 USB master port (only on CMC III Processing Unit)
- 8 Socket for accessory modules (display unit, GSM unit or ISDN unit)



- 9 Socket for external temperature sensor
- 10 RJ 45 Ethernet interface with PoE
- 11 1st RJ 45 CAN bus connection for CMC III sensors (max. 16)
- 12 2nd RJ 45 CAN bus connection for CMC III sensors (max. 16)
- 13 24 V DC voltage supply (power pack connection)
- 14 24 V DC voltage supply (direct connection)
- 15 Alarm relay output (floating contact)

CMC III control units

CMC III I/O unit

CMC III unit for monitoring up to eight digital inputs and controlling up to four relays. The relays can be linked to measured values in the software so that they are actuated under certain circumstances.

This system can be used to monitor devices and forward messages.

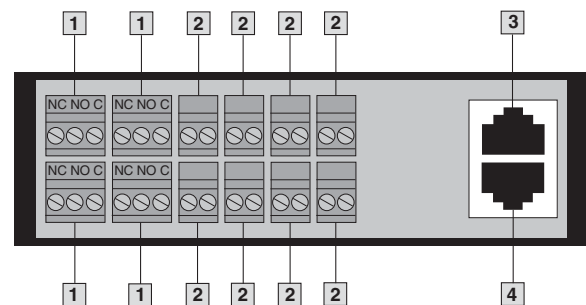
The CMC III I/O unit can not be run with the CMC III Processing Unit Compact.

- Max. number of CMC III Processing Units: 16
- Max. number of CMC III Processing Units Compact: –
- Digital input (terminal): 8 NC/NO
- Relay output (terminal): 4
- Changeover contact: Max. 24 V DC, 1 A
- RJ 45 CAN bus jacks: 2
- W x H x D: 138 x 40 x 120 + 12 mm front
- Colour: RAL 9005/7035

- 1 Relay outputs 1 – 4
- 2 Digital inputs 1 – 8
- 3 RJ 45 CAN bus connection
- 3 RJ 45 CAN bus connection



Connection information



CMC III Power Unit

CMC III unit with one input (C14) and two outputs (C13). The input is switched to the outputs via two relays. As a result, the outputs can be linked to measured values and therefore can be actuated automatically.

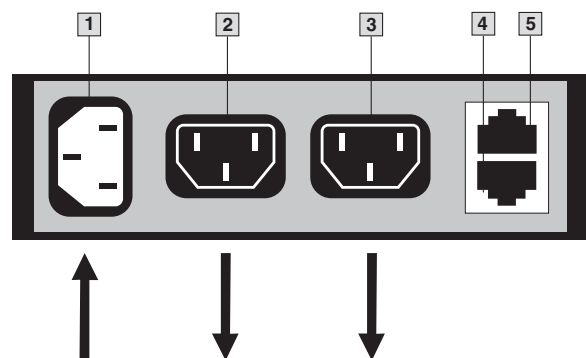
Examples of potential applications include fan regulation. Manual actuation is also possible using the CMC III operating interface. Each output is monitored individually, and various values are measured. Voltage, frequency, current, power and energy are measured for each output. The CMC III Power Unit can not be run with the CMC III Processing Unit Compact.

- Max. number of CMC III Processing Units: 16
- Max. number of CMC III Processing Units Compact: –
- Voltage measurement range: 100 – 230 V, 50/60Hz
- Frequency measurement range: 0 – 60 Hz
- Current measurement range: 200 mA – 10 A
- Power measurement range: 46 W – 2.3 kW
- Energy measurement range: 0 – 100000 kWh
- Fuse: 10 A (1st output + 2nd output)
- RJ 45 CAN bus jacks: 2
- W x H x D: 138 x 40 x 120 + 12 mm front
- Colour: RAL 9005/7035

- 1 Input, C14 power supply
- 2 1st output, C13 power supply
- 3 2nd output, C13 power supply
- 3 RJ 45 CAN bus connection
- 3 RJ 45 CAN bus connection



Connection information



CMC III sensors for direct connection



Temperature sensor

CMC III sensor with internal temperature sensor for in-airflow applications or alternatively with external temperature sensor for all application scenarios.

- Max. number of CMC III Processing Units: 32
- Max. number of CMC III Processing Units Compact: 4
- Measurement range of internal sensors: +0°C...+55°C
- Measurement range of external sensors: -40°C...+80°C
- Jack for external sensor: 1
- RJ 45 CAN bus jacks: 2
- W x H x D: 80 x 28 x 40 mm
- Colour: RAL 9005/7035



Temperature/humidity sensor

CMC III sensor with temperature sensor and humidity sensor in the enclosure front.

- Max. number of CMC III Processing Units: 32
- Max. number of CMC III Processing Units Compact: 4
- Temperature measurement range: +0°C...+55°C
- Relative humidity measurement range: 5 %...95 % RH
- RJ 45 CAN bus jacks: 2
- W x H x D: 80 x 28 x 40 mm
- Colour: RAL 9005/7035



Infrared access sensor

CMC III sensor with infrared transmitter and receiver for monitoring doors or side panels.

- Max. number of CMC III Processing Units: 32
- Max. number of CMC III Processing Units Compact: 4
- Transmitter: Infrared diode
- Receiver: Infrared receiver
- RJ 45 CAN bus jacks: 2
- W x H x D: 80 x 28 x 40 mm
- Colour: RAL 9005/7035



Vandalism sensor

CMC III sensor with integrated acceleration sensor for monitoring the three axes of movement.

- Max. number of CMC III Processing Units: 32
- Max. number of CMC III Processing Units Compact: 4
- Monitoring: x, y and z axes
- Measurement range: -2/4/8...+2/4/8 g
- Resolution: 0.1 g
- RJ 45 CAN bus jacks: 2
- W x H x D: 80 x 28 x 40 mm
- Colour: RAL 9005/7035

CMC III sensors for direct connection

Analogue airflow sensor

CMC III sensor with analogue sensor for measuring air speed, e.g. for fan monitoring.

- Max. number of CMC III Processing Units: 10
- Max. number of CMC III Processing Units with power supply via PoE: 5
- Max. number of CMC III Processing Units Compact: 4
- Sensor interface: 4 – 20 mA
- Measurement range: 0.5 to 10 m/s
- RJ 45 CAN bus jacks: 2
- Terminals for airflow sensor: 1
- W x H x D: 110 x 30 x 40 mm
- Colour: RAL 9005/7035



Analogue differential pressure sensor

CMC III sensor with analogue pressure sensor for monitoring a pressure differential, e.g. for climate-control applications. Tubing included in the scope of supply can be used to specify two points in the room where pressure is measured. The difference between these two pressure measurements is depicted as the measured value and monitored.

- Max. number of CMC III Processing Units: 32
- Max. number of CMC III Processing Units Compact: 4
- Pressure measurement points: 2
- Measurement range: -500...+500 Pa
- RJ 45 CAN bus jacks: 2
- W x H x D: 110 x 30 x 40 mm
- Colour: RAL 9005/7035



Universal sensor

CMC III sensor for connecting an external sensor. This sensor has a total of three connection terminals. Two of these terminals can be defined as digital inputs, S0 bus counters or a Wiegand interface for connecting external access monitoring systems. The third connection is an analogue interface for an external signal between 4 and 20 mA.

- Max. number of CMC III Processing Units: 32
- Max. number of CMC III Processing Units Compact: 4
- RJ 45 CAN bus jacks: 2
- W x H x D: 110 x 30 x 40 mm
- Colour: RAL 9005/7035

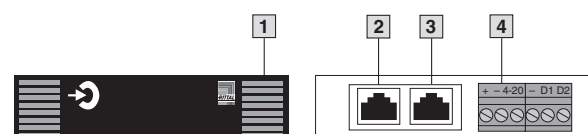
- 1 Multi-LED for the status display
- 2 RJ 45 CAN bus connection
- 3 RJ 45 CAN bus connection
- 4 Universal interface

Pin assignment to terminal 4:

- Pin 1 = output + 24 V DC
- Pin 2 = GND output
- Pin 3 = 4 – 20 mA input
- Pin 4 = 4 – 20 mA GND
- Pin 5 = digital input 1
- Pin 6 = digital input 2



Connection information



CMC III sensors for direct connection



CMC III smoke alarm

The CMC III smoke alarm is fitted at the top of the enclosure and monitors the air inside the enclosure for smoke particles. Settings can be made via the CMC III Processing Unit.

- Max. number of CMC III Processing Units: 32
- Max. number of CMC III Processing Units Compact: 4
- Measuring method: Silicon PIN photodiode/GaAs infrared LED
- RJ 45 CAN bus jacks: 2
- Diameter: 100 mm
- H: 50 mm
- Colour: White



CMC III leak sensor

The CMC III leak sensor has an external sensor mounted so that the contacts are pointing vertically down to the floor. These two contacts monitor a point on the floor for liquids (leakage). Settings can be made via the CMC III Processing Unit.

- Max. number of CMC III Processing Units: 32
- Max. number of CMC III Processing Units Compact: 4
- Measuring method: Conductivity measurement
- RJ 45 CAN bus jacks: 2
- Terminals for leak sensors: 1
- W x H x D: 110 x 30 x 40 mm
- Colour: RAL 9005/7035



CMC III leak sensor, 15 m

The CMC III leak sensor monitors a larger area of the floor for leaks. As soon as the 15 metre-long detection cable comes into contact with liquids, the sensor issues an alarm signal to indicate where on the floor the leak is. Settings can be made via the CMC III Processing Unit.

- Max. number of CMC III Processing Units: 32
- Max. number of CMC III Processing Units Compact: 4
- Measuring method: Conductivity measurement
- RJ 45 CAN bus jacks: 2
- Terminals for leak cable: 1
- Length of leak cable: 15 m
- W x H x D: 110 x 30 x 40 mm
- Colour: RAL 9005/7035

CMC III interface modules

CMC III CAN bus sensor

The CMC III CAN bus sensor supports the connection of selected sensors from the CMC-TC system to the new CMC III, allowing old applications to be upgraded with the CMC III Processing Unit / Compact. As well as the two CAN bus connections, the unit also has another connection for one of the old sensors. In this way, the unit functions as an interface between the old sensor and the new Processing Unit, and adapts the sensor data to the CAN bus protocol.

- Max. number of CMC III Processing Units: 32
- Max. number of CMC III Processing Units Compact: 4
- RJ 12 interfaces: 1 CMC-TC sensor
- RJ 45 CAN bus jacks: 2
- W x H x D: 110 x 30 x 40 mm
- Colour: RAL 9005/7035

The following CMC-TC sensors can be connected to the CMC III CAN bus sensor unit:

- Max. 1 x temperature sensor
- Max. 1 x analogue input 4 – 20 mA
- Max. 5 x access sensors in series
- Max. 1 x airflow sensor
- Max. 1 x smoke alarm
- Max. 1 x motion detector
- Max. 1 x digital input
- Max. 1 x digital relay output
- Max. 1 x voltage monitor
- Max. 1 x 48 V voltage sensor
- Max. 1 x leak sensor
- Max. 1 x leak sensor, 15 m
- Max. 1 x door control unit¹⁾
- Max. 1 x DET-AC extinguishing system²⁾
- Max. 1 x DET-AC early fire detection²⁾

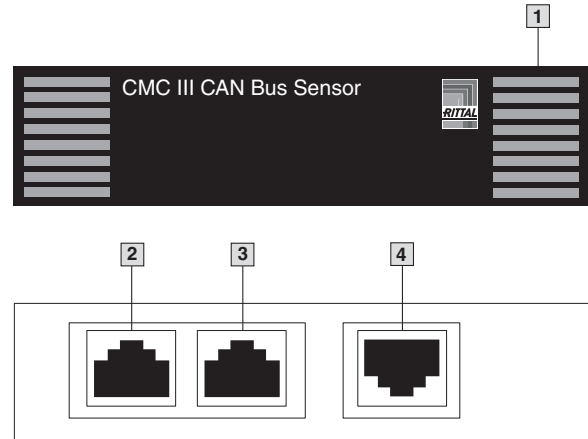
¹⁾ The device has two connections.

²⁾ The device has three connections.

- ❶ Multi-LED for the status display
- ❷ RJ 45 CAN bus connection
- ❸ RJ 45 CAN bus connection
- ❹ Connection for CMC-TC sensor, RJ 12



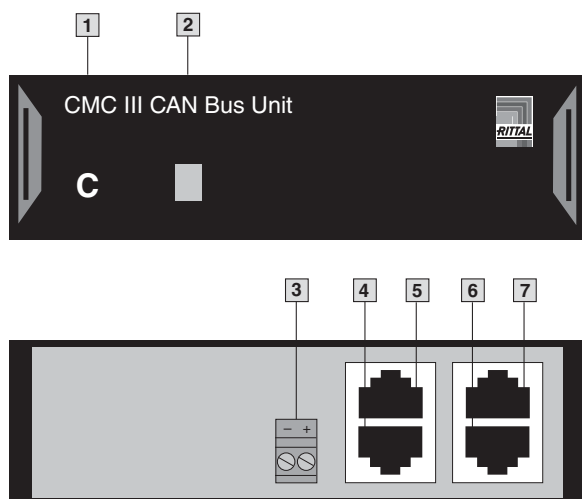
Connection information



CMC III interface modules



Connection information



CMC III CAN Bus unit

The CMC III CAN bus unit acts as an interface between the CMC III Processing Unit and the PSM measurement bars and modules.

The unit has four connections: Two connections represent the interface to the CAN bus and to the other CMC III sensors, while up to four PSM modules (i.e. a total of up to eight PSM modules per CMC III CAN bus unit) or one measurement bar can be connected to each of the other two connections.

When connecting PSM modules, the CMC III CAN bus unit must be externally supplied with 24 V via terminals.

- Max. number of CMC III Processing Units: 4
- Max. number of CMC III Processing Units with power supply via PoE: 1
- Max. number of CMC III Processing Units Compact: 1
- RJ 45 interfaces: 2 CMC-TC units
- RJ 45 CAN bus jacks: 2
- W x H x D: 138 x 40 x 120 + 12 mm front
- Colour: RAL 9005/7035

The following sensors can be connected to the CMC III CAN bus unit:

- Max. 2 x FCS fan control systems
- Max. 2 x FCS fan mounting plates DC
- Max. 2 x 4 x PCU, various active modules
- Max. 2 x 4 x active PSM, various active modules
- Max. 2 x PSM busbars, 16 A
- Max. 2 x PSM busbars, 32 A
- Max. 2 x PSM measurement module, 16 A

- 1 "C" button for acknowledging notifications
- 2 Multi-LED for the status display
- 3 Voltage supply (direct connection)
- 4 RJ 45 connection for CMC-TC unit
- 5 RJ 45 connection for CMC-TC unit
- 6 RJ 45 CAN bus connection
- 7 RJ 45 CAN bus connection

CMC III access control

CMC III CAN bus access

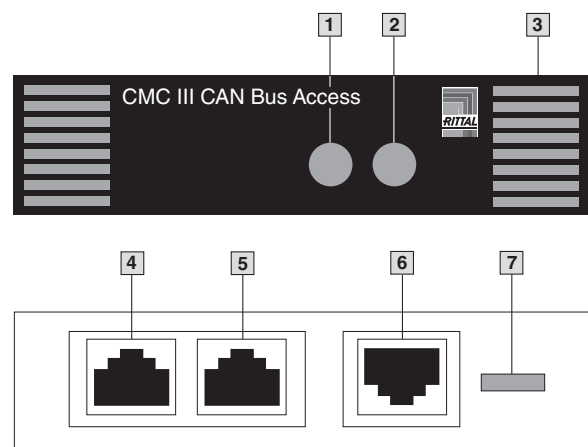
CMC III unit for controlling and monitoring access to enclosures. One handle and one reader unit can be connected to each CMC III CAN bus access. The handles can be linked to various numerical codes or RFID card numbers via the CMC III Processing Unit / Compact website, which means that all the handles connected to a CMC III Processing Unit / Compact can be controlled with just one reader unit. The integral infrared sensor also ensures that the status of the controlled door (open/closed) is monitored.

- Max. number of CMC III Processing Units: 16
- Max. number of CMC III Processing Units with power supply via PoE: 5
- Max. number of CMC III Processing Units Compact: 4
- Transmitter: Infrared diode
- Receiver: Infrared receiver
- Interfaces: 1 CMC III reader unit
- RJ 12 interfaces: 1 handle (electromechanical)
- RJ 45 CAN bus jacks: 2
- W x H x D: 110 x 30 x 40 mm
- Colour: RAL 9005/7035

- 1 Infrared receiver
- 2 Infrared diode (transmitter)
- 3 Multi-LED for status display
- 3 RJ 45 CAN bus connection
- 3 RJ 45 CAN bus connection
- 4 Connection for handle, RJ 12
- 7 Connection for CMC III reader unit



Connection information



CMC III coded lock

The CMC III coded lock is connected to the CMC III CAN bus access. Any amount of eight-digit number combinations can be entered and linked with handles.

- Numerical code: 00000000 – 99999999 (variable)
- Connection cable: 3 m
- W x H x D: 50 x 190 x 25 mm
- Colour: RAL 7035



CMC III transponder reader

The CMC III transponder reader is connected to the CMC III CAN bus access. By contactlessly holding a transponder card in front of it, authorisation (UID of the card) is checked in the CMC III Processing Unit / Compact, and the corresponding door(s) is/are released.

- Technology: Transponder 13.56 MHz
- Tags: ISO 14443A, ISO 14443B, ISO 15693, ISO 18000-3, Mifare
- Connection cable: 3 m
- W x H x D: 50 x 190 x 25 mm
- Colour: RAL 7035



CMC III

access control



Electromagnetic handle

The handle locks the door and monitors the lever. It can always be opened independently of the control system using the master key. A semi-cylinder (lock insert, lock No. 3524 E) is included in the scope of supply, but a semi-cylinder with an overall length of 40 mm to DIN 18 254 can also be used.

A CAN bus access (DK 7030.200) must be fitted on the rack frame for each handle. This device has an integrated infrared access sensor and the handle and a reader unit can be connected.

If the lever handle is closed, the locking mechanism integrated into the handle latches automatically. The handle can be released via the CMC III system in the network or via optional add-on systems, such as Mifare transponder readers. The handle locks without consuming any voltage (no electrical connection). Once the electrical release has been issued, the push-button can be pressed to release the lever. The enclosure must be opened within a specified period of time that is set in the CMC III. Using the key to open the enclosure always overrides all other methods, i.e. the enclosure can always be opened with the key when electrically locked and in the event of a power failure (emergency opening).

Technical specifications:

- Rated voltage: 24 V DC
- Rated current: max. 100 mA
- Connection cable: Length 3 m, RJ 12 connector
- Temperature application range: +5°C to +40°C
- Protection category: IP 40

CMC III accessories

CMC III power pack

The CMC III power pack operates with an input voltage of 100 – 240 V, 50/60 Hz and supplies 24 V. It is specifically tailored to the CMC III design and can be positioned in a CMC III mounting unit. As well as a special connector for the CMC III Processing Unit / Compact, there are also two further terminals available as 24 V outputs.

- Input: C14, 100 – 230 V, 50/60 Hz
- Output: 24 V DC, 2 A
- W x H x D: 138 x 40 x 120 + 12 mm front
- Colour: RAL 9005/7035



CMC III programming cable USB

The CMC III programming cable is used the first time the CMC III Processing Unit starts up. During initial start-up, the programming cable connects the CMC III Processing Unit / Compact to the USB interface of a PC. A driver for Windows systems is also included in the scope of supply and must be installed on the PC.

- Connector 1: USB, series A (for laptops)
- Connector 2: Mini USB (for CMC III Processing Unit / Compact)
- Length: 3 m



CMC III RJ 45 CAN bus connection cable

The CMC III CAN bus connection cables are used to connect sensors to each other and to the CMC III Processing Unit / Compact. As they are available in different lengths, the CMC III system can be adapted to various applications and built to a custom design.

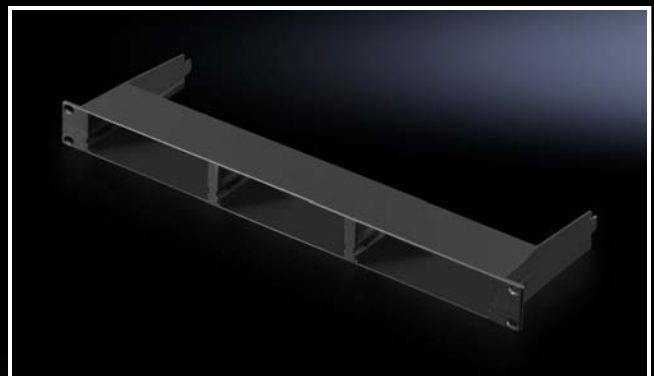
- Connector 1/2: RJ 45
- Lengths: 0.5 m – 10 m



CMC III mounting unit

The CMC III mounting units make it easier to install CMC III units in network and server enclosures. There are two different mounting units – one for installation in the 19" section (encompasses three CMC III units) and one for installation on the enclosure frame. Click and snap-in fixings make installation and subsequent maintenance work easier.

- CMC III mounting unit, 1 U:
W x H x D: 19" x 1 U x 141 mm
- CMC III mounting unit for enclosure frame:
W x H x D: 170 x 50 x 160 mm



CMC III accessories



CMC III GSM unit

A module for a redundant alarm signal can be connected to each CMC III Processing Unit / Compact. The GSM unit quad-band forwards the alarm notifications as an SMS to up to 16 recipients via GSM.

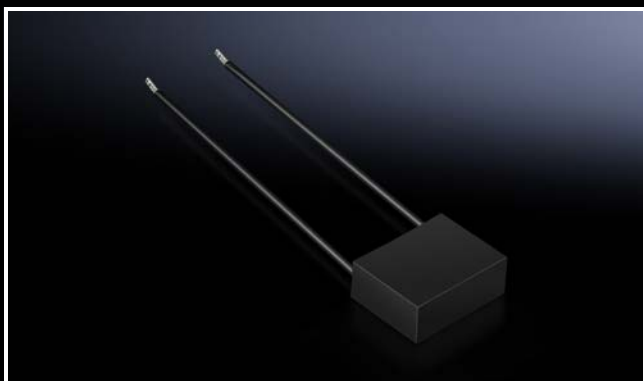
- Frequency range: 850/900/1800/1900 MHz
- W x H x D: 138 x 40 x 120 mm
- Front: 12 mm



CMC III ISDN unit

A module for a redundant alarm signal can be connected to each CMC III Processing Unit / Compact. The ISDN unit forwards the alarm notifications as an SMS to up to 16 recipients via ISDN.

- DSS1 (Euro-ISDN)
- W x H x D: 138 x 40 x 120 mm
- Front: 12 mm



CMC III interference suppressor for fans

When using the Power Unit, it is important to suppress interference from the fan motors that it operates. To do this, the interference suppressors for each fan must be connected directly to the motor. Each interference suppressor incorporates a capacitor and a resistor.



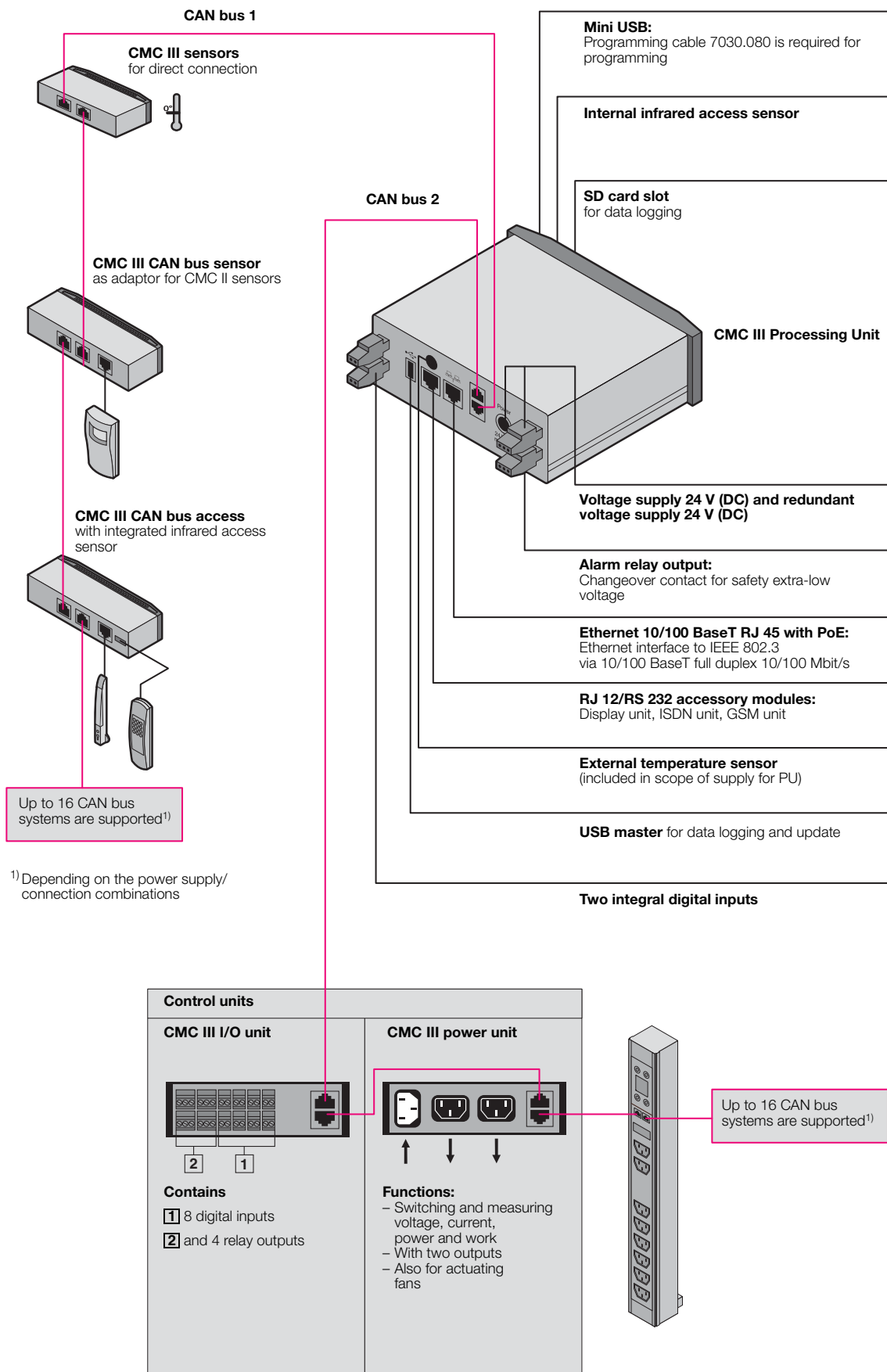
CMC III cable clamp straps

For securing to the rear of the CMC III 19" mounting unit. Enables tidy cable routing behind the built-in CMC III devices and can be used to attach cables for strain relief purposes. Cables can easily be laid in a loop to allow the built-in CMC III devices to be removed from the mounting unit without the need for tools.

CMC III – monitoring system

CMC III Processing Unit

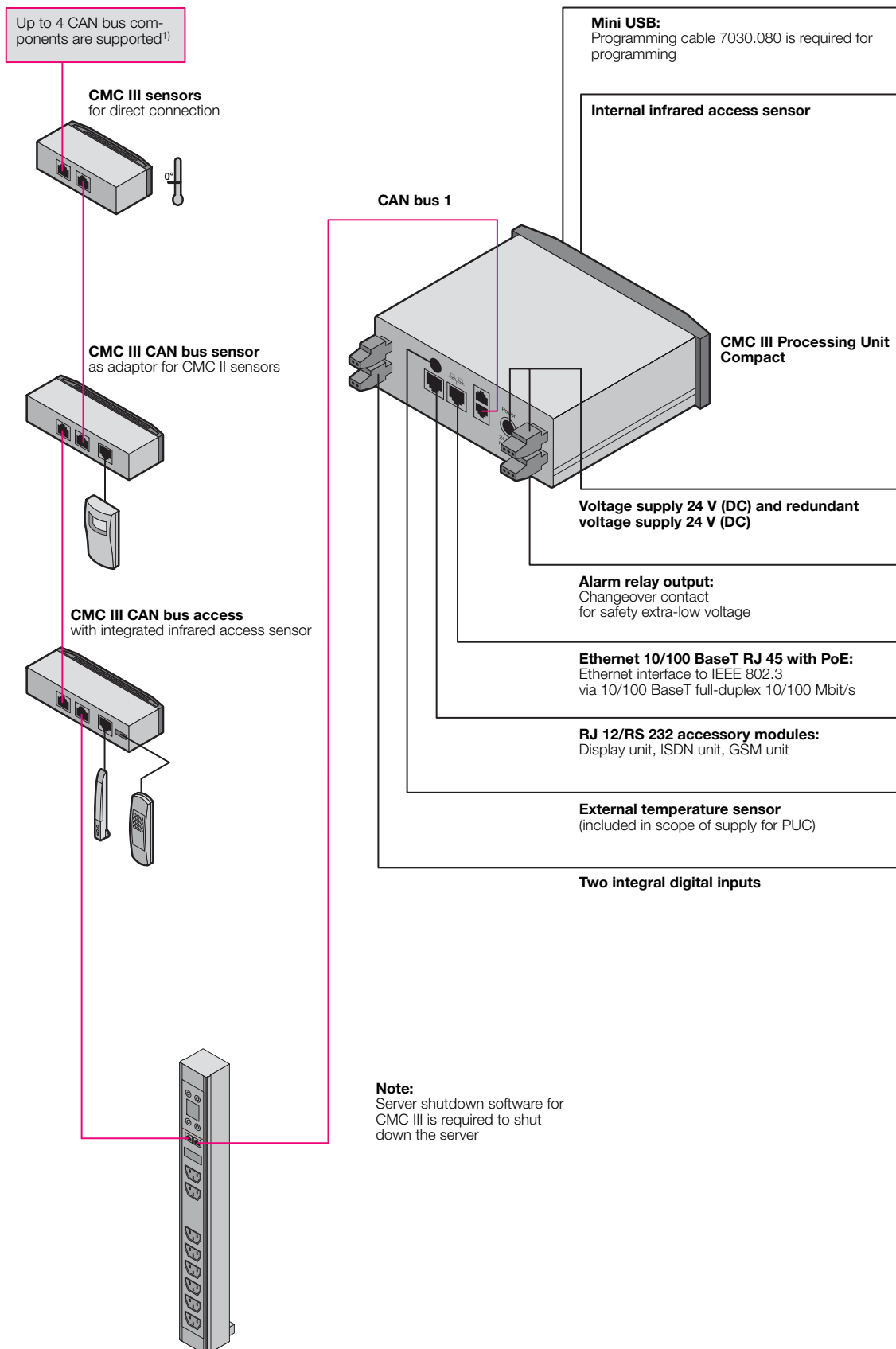
System overview



¹⁾ Depending on the power supply/
connection combinations

CMC III – monitoring system

CMC III Processing Unit Compact System overview



Rittal – The System.

Faster – better – everywhere.

- Enclosures
- Power Distribution
- Climate Control
- IT Infrastructure
- Software & Services

You can find the contact details of all
Rittal companies throughout the world here.



www.rittal.com/contact

XVW000085ENT1603

ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

IT INFRASTRUCTURE

SOFTWARE & SERVICES



FRIEDHELM LOH GROUP

ATTACHMENT 1 – CATALOGUE AND DATASHEET

NETWORKING



Main

Range of product	ConneXium
Product or component type	Ethernet TCP/IP managed switch
Concept	Transparent Ready
Communication port protocol	Ethernet TCP/IP
Port Ethernet	100BASE-FX - 2 port(s) fiber optic 10BASE-T/100BASE-TX - 14 port(s) copper cable
Maximum number of switches in cascade	Unlimited

Complementary

Integrated connection type	Duplex SC fiber optic Shielded RJ45 copper cable
Transmission support medium	Single mode optical fiber for copper cable Twisted shielded pairs cable CAT 5E for fiber optic
Cable distance between devices	100 m copper cable
Optic fiber length	9/125 µm
Attenuation	16 dB 9/125 µm
Ethernet service	Secure port Configuration via web server Rapid Spanning Tree Protocol (RSTP) IGMP Snooping VLAN Data stream control SNTP client Multicast filtering SMTP V3 FDR Priority port
Maximum number of switches in a ring	50
Redundancy	Redundant power supplies Redundant single ring Ring coupling
[Us] rated supply voltage	24 V
Supply voltage limits	18...30 V AC SELV 9.6...60 V DC SELV
Power consumption in W	11.8 W


Disclaimer: This documentation is not intended as a substitute for and is not to be used for determining suitability or reliability of these products for specific user applications

Electrical connection	Removable connector 6 ways power supply
Mounting support	35 mm symmetrical DIN rail
Marking	CE
Local signalling	1 LED fault 2 LEDs P1 P2 power supplies 1 LED ring manager 1 LED stand-by 1 LED per channel copper port activity 1 LED per channel copper port status
Alarm output	1 voltfree contact ≤ 1 A
Alarm function	Data link status Redundancy ring fault Switch fault Power supply fault
Ethernet cabling system	TF switches
Width	111 mm
Height	131 mm
Depth	111 mm
Product weight	0.6 kg

Environment

Ambient air temperature for operation	0...60 °C
Relative humidity	> 0...95 % without condensation
IP degree of protection	IP20
Standards	EN/IEC 61131-2 UL 1604 Class 1 Division 2 UL 508 CSA C22.2 No 214 CSA C22.2 No 213 Class I Division 2
Product certifications	C-Tick GL

Offer Sustainability

Sustainable offer status	Not Green Premium product
RoHS (date code: YYWW)	Compliant - since 1050 - Schneider Electric declaration of conformity  Schneider Electric declaration of conformity

Contractual warranty

Warranty period	18 months
-----------------	-----------

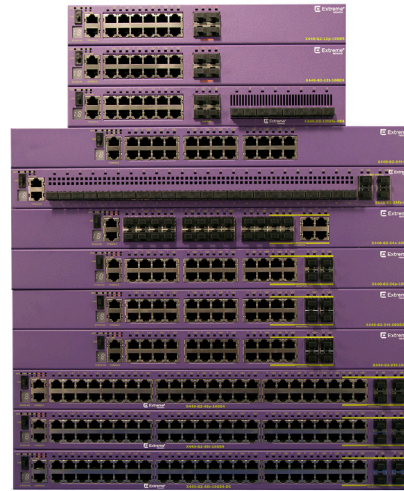
Highlights

Hardware Models

- 12, 24, and 48-port GbE models
- 4 x 1GbE available uplink ports upgradeable to 10GbE via software license (except for extended temperature models)
- SFP, Copper PoE-Plus, non-PoE and 100Base-FX models
- Extended 0°C to 60°C operating range models
- Two SummitStack-V stacking ports (except for extended temperature models) enable up to 8 switches to be stacked together
- All configurations non-blocking full duplex
- 10GbE LRM support on 48-port switch models

Features

- Side-to-side, left-to-right airflow
- Fixed power supplies, along with RPS
- Full PoE-Plus 30W power on 48-port models
- DC Power option
- Energy Efficient Ethernet
- 10MB/100MB half-duplex support
- Role-based policy capabilities allow individualized access to specific applications or services
- ExtremeCloud™ cloud-based management on select models
- Extreme Management Center Support



ExtremeSwitching™ X440-G2

Scalable Cost-Effective Edge Switch with ExtremeXOS Modular Operating System

Product Overview

The ExtremeSwitching X440-G2 series is a scalable cost-effective family of edge switches powered by Extreme Networks ExtremeXOS, a highly resilient OS providing continuous uptime, manageability and operational efficiency. The X440-G2 series switches provide high-performance routing and switching, flexible stacking, PoE-plus support and comprehensive security, while extending the benefits of ExtremeXOS to the campus edge.

The X440-G2 Series easy-to-use, yet powerful, management services include role-based policies for controlled access to specific network applications. Select X440-G2 Series switches can also be cloud-managed via ExtremeCloud™, Extreme Networks innovative single-pane subscription-based management solution.

Intelligent Switching

The X440-G2 Series supports sophisticated and intelligent Layer 2 switching, as well as Layer 3 IPv4/IPv6 routing. They also support role-based policy capabilities, Provider Bridges, bidirectional Access Control Lists, as well as granular (8 Kbps) ingress/egress bandwidth control. Altogether, these enable fine-grained control over traffic flows, as well as controlled access to specific network services and application.

Flexible 10GBE Port Upgrades

All X440-G2 base models come equipped with 4 upgradeable 1GbE ports, resident on either the faceplate or rear panel of each model. These 1GbE ports can be upgraded to 10GbE Ethernet via a simple software license. This gives administrators the option to increase switch uplink speeds without replacing the entire switch.

Notes: 10GbE upgrades are not supported on extended temperature models. The two rear-panel 1GbE copper combo ports on the 48 port switches become 10GBase-T ports when either 10GbE license is applied to the rear-panel SFP/SFP+ ports.

High-Performance Stacking

ExtremeXOS SummitStack-V capabilities allow up to eight X440-G2 switches to be stacked together via two of the native X440-G2 stacking ports. SummitStack-V allows use of standard 10Gb Ethernet cabling and optics technologies, providing longdistance stacking connectivity of up to 40 Km while eliminating the cable complexity of non-standard stacking options. X440-G2 switches can be stacked with other X450-G2, X460-G2, X670-G2 and X770 switches via SummitStack-V so long as all are running the same version of ExtremeXOS.

Note 1: SummitStack-V uses two of the four available uplink ports on the X440-G2 and runs a 10Gb non-Ethernet stacking protocol. These stacking ports DO NOT require a 10GbE software license, and can take full advantage of standard SFP+ transceivers.

Note 2: Extended temperature range switches do not support stacking.

IEEE 802.3AT Poe-Plus

X440-G2 Series switches support both IEEE 802.3at PoE-Plus and IEEE 802.3af PoE to enable connection of standards compliant PoE devices today and into the future. Power over Ethernet allows connection of Ethernet-powered devices, such as wireless access points, Voice over IP phones, and security cameras. The X440-G2 can also support full PoE-Plus 30W power across all 48 ports with an external redundant power supply (RPS).

Role-Based Policy

The X440-G2 supports role-based policies that can be centrally administered through the ExtremeManagement (formerly Netsight) policy manager. This policy framework empowers network administrators to define distinct roles or profiles to represent industry-specific operational groups that may exist in an education or a business environment (e.g., administrator, teacher, student, guest). Each defined role can then be granted individualized access to specific network services and applications and these access privileges remain associated with users as they move across both wired and wireless network access points.

ExtremeCloud™ Management

Provides a single plane of glass for cloud managing both the wired and wireless components of your network. Zero touch provisioning also significantly reduces deployment

times. Select X440-G2 models have been enabled for use with ExtremeCloud. See the ExtremeCloud Data Sheet for details.

USB 2.0 Support

All X440-G2 switches have a USB 2.0 port that is supported as a port to a storage device for all EXOS versions of 22.1 or higher.

Extended Temperature Range Support

The X440-G2 include three switch models that support 0°C to 60°C operating range (Models 16539, 16540 and 16541) to address the unique environmental needs of specific industries and/or locations.

Comprehensive Security Management

The X440-G2 provides comprehensive security, including:

- User policy and host integrity enforcement, and identity management.
- Universal Port Dynamic Security Profiles for fine granular security policies across the network.
- Threat detection and response instrumentation to react to network intrusion.
- Denial of Service (DoS) protection and IP security against man-in-the-middle and DoS attacks.

These features ensure both the security of the network and of users accessing the network.

Audio Video Bridging (AVB)

The X440-G2 series supports IEEE 802.1 Audio Video Bridging to enable reliable, real-time audio/video transmission over Ethernet. AVB technology delivers the quality of service required for today's high-definition and time-sensitive multimedia streams.

Note: Only 24 ports on either the 24 or 48 port models support AVB.

Ordering Notes

All X440-G2 switches ship with fixed fans and power supplies:

- All the X440-G2 switches support optional external redundant power supplies (RPS).
- The following three switch models that support 0C to 60C are NOT upgradeable to 10GbE:
 - X440-G2-24fx-GE4
 - X440-G2-12t8fx-GE4
 - X440-G2-24t-GE4

Specifications

Switch Model	Maximum 10/100/1000 Base-T Ports	Maximum Active 1Gb SFP Ports	Maximum 10Gb SFP+ Ports	Aggregated Switch Bandwidth*	Frame Forwarding Rate*
X440-G2-12t-10GE4	12	4	4 via license	104 GBPS	77.4 MPPS
X440-G2-24t-10GE4	24	8 (4 + 4 Combo)	4 via license	128 GBPS	95.2 MPPS
X440-G2-48t-10GE4	48	8 (2 + 6 Combo)	4 via license	176 GBPS	130.9 MPPS
X440-G2-12p-10GE4	12	4	4 via license	104 GBPS	77.4 MPPS
X440-G2-24p-10GE4	24	8 (4 + 4 Combo)	4 via license	128 GBPS	95.2 MPPS
X440-G2-48p-10GE4	48	8 (2 + 6 Combo)	4 via license	176 GBPS	130.9 MPPS
X440-G2-24t-10GE4-DC	24	8 (4 + 4 Combo)	4 via license	128 GBPS	95.2 MPPS
X440-G2-48t-10GE4-DC	48	8 (2 + 6 Combo)	4 via license ¹	176 GBPS	130.9 MPPS
X440-G2-24x-10GE4	4 Combo	28 (24 + 4 Combo)	4 via license	128 GBPS	95.2 MPPS
X440-G2-24fx-GE4	24 100 Base-FX	4	0	12.8 GBPS	9.5 MPPS
X440-G2-12t8fx-GE4	12 10/100/1000 + 8 100 Base-FX	4	0	33.6 GBPS	25.0 MPPS
X440-G2-24t-GE4	24 10/100/1000	4	0	56 GBPS	41.7 MPPS

¹ 2 10GBase-T combo ports

*-with 10Gb licenses if available with license

- Less than 4 microsecond latency (64-byte)
- Layer 2/MAC Addresses: 16K
- IPv4 LPM Entries: 480
- IPv4 Hosts: 1000
- IPv6 LPM (64-bit) Entries: 240
- 4092 user-created VLAN/VMANs
- 9216 Byte Max Packet Size (Jumbo Frame)
- 128 load sharing trunks, up to 8 members per trunk
- 1,024 ingress bandwidth meters, 256 egress meters
- Ingress and egress bandwidth policing/rate limiting per flow/ACL
- 8 QoS egress queues/port
- Egress bandwidth rate shaping per egress queue and per port.
- Rate Limiting Granularity: 8 Kbps
- Half-duplex 10/100 supported on the following 10/100/1000 ports:
 - 12 port switches: Ports 1-12
 - 24 port switches: Ports 1-16
 - 48 port switches: Ports 1-16 and Ports 25-40
- LRM support on rear-panel SFP/SFP+ ports on all 48-port switches
- Policy Capabilities
 - Policy Profiles: 63
 - Rules per Profile: Up to 440
 - Authenticated Policy Users per Switch: Up to 1,536
 - Authenticated Policy Users per Port: Up to 1,536
 - Unique Permit/Deny Rules per switch: 440
 - MAC Rules: N/A
 - IPv4 Rules: 256
 - IPv6 Rules: N/A
 - L2 Rules: 184
- Rate Limiting: Per Class of Service

Specifications (Cont.)

Switch Hardware	Ports
X440-G2-12t-10GE4	<ul style="list-style-type: none"> • 12 x 10/100/1000BASE-T (RJ-45) • 4 x 1GBASE-X SFP (unpopulated front-panel ports) upgradeable to 10Gb Ethernet via licensing • 1 x Serial (console port RJ-45) with RTS/CTS modem control • 1 x 10/100/1000BASE-T out-of-band management port • Coaxial Barrel Connector RPS port
X440-G2-24t-10GE4	<ul style="list-style-type: none"> • 24 x 10/100/1000BASE-T (RJ-45) • 4 x 1GBASE-X SFP (unpopulated) combo ports • 4 x 1GBASE-X SFP (unpopulated rear-panel ports) upgradeable to 10Gb Ethernet via licensing • 1 x Serial (console port RJ-45) with RTS/CTS modem control • 1 x 10/100/1000BASE-T out-of-band management port • 2x7 RPS port
X440-G2-48t-10GE4	<ul style="list-style-type: none"> • 48 x 10/100/1000BASE-T (RJ-45) • 4 x 1GBASE-X SFP (unpopulated) combo ports • 2 x 1GbE copper combo ports upgradable to 10GbE on rear-panel • 4 x 1GBASE-X SFP (unpopulated rear-panel ports) upgradeable to 10Gb Ethernet via licensing • 1 x Serial (console port RJ-45) with RTS/CTS modem control • 1 x 10/100/1000BASE-T out-of-band management port • 2x7 RPS port
X440-G2-12p-10GE4	<ul style="list-style-type: none"> • 12 x 10/100/1000BASE-T PoE-Plus • 4 x 1GBASE-X SFP (unpopulated front-panel ports) upgradeable to 10Gb Ethernet via licensing • 1 x Serial (console port RJ-45) with RTS/CTS modem control • 1 x 10/100/1000BASE-T out-of-band management port • 2x7 RPS port
X440-G2-24p-10GE4	<ul style="list-style-type: none"> • 24 x 10/100/1000BASE-T PoE-Plus • 4 x 1GBASE-X SFP (unpopulated) combo ports • 4 x 1GBASE-X SFP (unpopulated rear-panel ports) upgradeable to 10Gb Ethernet via licensing • 1 x Serial (console port RJ-45) with RTS/CTS modem control • 1 x 10/100/1000BASE-T out-of-band management port • 2x7 RPS port
X440-G2-48p-10GE4	<ul style="list-style-type: none"> • 48 x 10/100/1000BASE-T PoE-Plus • 4 x 1GBASE-X SFP (unpopulated) combo ports • 2 x 1GbE copper combo ports upgradable to 10GbE on rear-panel • 4 x 1GBASE-X SFP (unpopulated rear-panel ports) upgradeable to 10Gb Ethernet via licensing • 1 x Serial (console port RJ-45) with RTS/CTS modem control • 1 x 10/100/1000BASE-T out-of-band management port • 2x9 RPS port
X440-G2-24t-10GE4-DC	<ul style="list-style-type: none"> • 24 x 10/100/1000BASE-T (RJ-45) • 4 x 1GBASE-X SFP (unpopulated) combo ports • 4 x 1GBASE-X SFP (unpopulated rear-panel ports) upgradeable to 10Gb Ethernet via licensing • 1 x Serial (console port RJ-45) with RTS/CTS modem control • 1 x 10/100/1000BASE-T out-of-band management port • 2x7 RPS port
X440-G2-48t-10GE4-DC	<ul style="list-style-type: none"> • 48 x 10/100/1000BASE-T (RJ-45) • 4 x 1GBASE-X SFP (unpopulated) combo ports • 2 x 1GbE copper combo ports upgradable to 10GbE on rear-panel • 4 x 1GBASE-X SFP (unpopulated rear-panel ports) upgradeable to 10Gb Ethernet via licensing • 1 x Serial (console port RJ-45) with RTS/CTS modem control • 1 x 10/100/1000BASE-T out-of-band management port • 2x7 RPS port
X440-G2-24x-10GE4	<ul style="list-style-type: none"> • 24 x SFP (unpopulated) • 4 x 10/100/1000 combo ports • 4 x 1GBASE-X SFP (unpopulated rear-panel ports) upgradeable to 10Gb Ethernet via licensing • 1 x Serial (console port RJ-45) with RTS/CTS modem control • 1 x 10/100/1000BASE-T out-of-band management port • 2x7 RPS port

Specifications (Cont.)

Switch Hardware	Ports
X440-G2-24fx-GE4	<ul style="list-style-type: none"> 24 x 100Base-FX – LC connectors 4 x 1GBASE-X SFP (unpopulated front-panel ports) 1 x Serial (console port RJ-45) with RTS/CTS modem control 1 x 10/100/1000BASE-T out-of-band management port 2x7 RPS port
X440-G2-12t8fx-GE4	<ul style="list-style-type: none"> 12 x 10/100/1000BASE-T with 8 x 100Base-FX – LC connectors 4 x 1GBASE-X SFP (unpopulated front-panel ports) 1 x Serial (console port RJ-45) with RTS/CTS modem control 1 x 10/100/1000BASE-T out-of-band management port 2x7 RPS port
X440-G2-24t-GE4	<ul style="list-style-type: none"> 24 x 10/100/1000BASE-T (RJ-45) 4 x 1GBASE-X SFP (unpopulated rear-panel ports) 1 x Serial (console port RJ-45) with RTS/CTS modem control 1 x 10/100/1000BASE-T out-of-band management port 2x7 RPS port

Physical

Switch Model	Weight	Height	Width	Depth
X440-G2-12t-10GE4	5.82 lb (2.64 kg)	1 RU / 1.73 inches (4.4 cm)	12.01 inches (30.5 cm)	10.28 inches (26.1 cm)
X440-G2-24t-10GE4	8.07 lb (3.66 kg)	1 RU / 1.73 inches (4.4 cm)	17.36 inches (44.1 cm)	10.01 inches (25.4 cm)
X440-G2-48t-10GE4	11.22 lb (5.09 kg)	1 RU / 1.73 inches (4.4 cm)	17.36 inches (44.1 cm)	14.51 inches (36.85 cm)
X440-G2-12p-10GE4	6.66 lb (3.02 kg)	1 RU / 1.73 inches (4.4 cm)	12.01 inches (30.5 cm)	10.28 inches (26.1 cm)
X440-G2-24p-10GE4	9.44 lb (4.28 kg)	1 RU / 1.73 inches (4.4 cm)	17.36 inches (44.1 cm)	10.01 inches (25.4 cm)
X440-G2-48p-10GE4	14.55 lb (6.60 kg)	1 RU / 1.73 inches (4.4 cm)	17.36 inches (44.1 cm)	14.51 inches (36.85 cm)
X440-G2-24t-10GE4-DC	8.07 lb (3.66 kg)	1 RU / 1.73 inches (4.4 cm)	17.36 inches (44.1 cm)	10.01 inches (25.4 cm)
X440-G2-48t-10GE4-DC	11.20 lb (5.08 kg)	1 RU / 1.73 inches (4.4 cm)	17.36 inches (44.1 cm)	14.51 inches (36.85 cm)
X440-G2-24x-10GE4	8.22 lb (3.73 kg)	1 RU / 1.73 inches (4.4 cm)	17.36 inches (44.1 cm)	10.01 inches (25.4 cm)
X440-G2-24fx-GE4	8.66 lb (3.93 kg)	1 RU / 1.73 inches (4.4 cm)	17.36 inches (44.1 cm)	10.01 inches (25.4 cm)
X440-G2-12t8fx-GE4	6.50 lb (2.95 kg)	1 RU / 1.73 inches (4.4 cm)	12.01 inches (30.5 cm)	10.28 inches (26.1 cm)
X440-G2-24t-GE4	7.98 lb (3.62 kg)	1 RU / 1.73 inches (4.4 cm)	17.36 inches (44.1 cm)	10.01 inches (25.4 cm)

CPU/Memory

- 64-bit MIPS Processor, 1 GHz clock, single core
- 1GB ECC DDR3 DRAM
- 4GB eMMC Flash
- 1.5MB packet buffer on 12 - 24 port switches, 3.0MB packet buffer on 48 port switches

LED Indicators

- Per port status LED including power status.
- System Status LEDs: management, fan and power.
- 7 segment display of stack number – operational on switches that support stacking.

Stacking

- SummitStack-V with support for up to eight switches per stack.
- Mixed stacking with other Extreme X-Series switches, so long as all are running the same ExtremeXOS version.
- Requires two of the four available X440-G2 uplink ports.

Note: SummitStack-V stacking is enabled on two of the four X440-G2 uplink ports by default (no license required). All stacking ports operate at 10Gb, but do not use standard Ethernet protocols. X440-G2 uplink ports, when not used for stacking, run the standard Ethernet protocol. Non-stacking uplink ports are limited by default

to 1GbE, unless upgraded via software license. 10GbE licenses are available, in both two- and four-port versions, as well as a license to upgrade a dual 10GbE uplink switch to a four 10GbE uplink switch, that enable X440-G2 uplink ports to run the 10Gb Ethernet protocol.

Mapping of the two default X440-G2 stacking ports to their respective physical chassis interface #'s — by chassis type — are listed below.

X440-G2 Switches*	Stack Port #	Physical Uplink Port # On Chassis
48 Port Models	1	49 (Rear Panel, Dedicated SFP+ Port)
	2	50 (rear panel, dedicated SFP+ port)
24 Port Models	1	27 (Rear Panel)
	2	28 (Rear Panel)
12 Port Models	1	15 (Front Panel)
	2	16 (Front Panel)

*The three extended temperature X440-G2 models (16539, 16540 and 16541) do NOT stack.

Power

Switch Model	Minimum ¹ Heat Dissipation (BTU/HR)	Minimum ¹ Power Consumption (Watts)	Maximum ² Heat Dissipation (BTU/HR)	Maximum ² Power Consumption (Watts)
X440-G2-12t-10GE4	52	15	109	32
X440-G2-24t-10GE4	87	26	136	40
X440-G2-48t-10GE4	141	41	208	61
X440-G2-12p-10GE4	72	21	216 (@200W PoE)	264
X440-G2-24p-10GE4	121	35	410 (@380W PoE)	500
X440-G2-48p-10GE4	196	53	755 (@740W PoE)	961
X440-G2-24t-10GE4-DC	77	23	134	39
X440-G2-48t-10GE4-DC	137	40	207	61
X440-G2-24x-10GE4	87	26	172	51
X440-G2-24fx-GE4	166	49	223	65
X440-G2-12t8fx-GE4	108	32	159	47
X440-G2-24t-GE4	76	22	130	38

¹ Idle no ports linked

² fans high all ports 100% traffic

The Non-PoE Extended Temperature Switches (X440-G2-24FX-GE4, X440-G2-12T8FX-GE4, X440-G2-24T-GE4)

	Fixed Internal Power Supply
Voltage Input Range	100 - 240 VAC†
Line Frequency Range	50 - 60 Hz +/- 5%
Power Supply Input Socket	IEC 320 C14
Power Cord Input Plug	IEC 320 C13
Operating Temperature	0° C to 60° C Normal Operation

The 12, 24, and 48 Port 10/100/1000 Models (Both PoE and Non-PoE)

	Fixed Internal Power Supply
Voltage Input Range	100 - 240 VAC†
Line Frequency Range	50 - 60 Hz +/- 5%
Power Supply Input Socket	IEC 320 C14
Power Cord Input Plug	IEC 320 C13
Operating Temperature	0° C to 50° C Normal Operation

† - The power supplies will continue to operate +/- 10% of the rated input to accommodate temporary loss of input voltage regulation.

Switch Model	Power Supply Input Socket	Power Cord Input Plug/Input Socket	Power Supply Cord Gauge	Redundant Power Supply Input Socket
X440-G2-12t-10GE4	IEC 320 C14	IEC 320 C13/C14	Min 18AWG/0.75mm ²	Coaxial Barrel Connector
X440-G2-24t-10GE4	IEC 320 C14	IEC 320 C13/C14	Min 18AWG/0.75mm ²	2x7 Terminal Block
X440-G2-48t-10GE4	IEC 320 C14	IEC 320 C13/C14	Min 18AWG/0.75mm ²	2x7 Terminal Block
X440-G2-12p-10GE4	IEC 320 C14	IEC 320 C13/C14	Min 18AWG/0.75mm ²	2x7 Terminal Block
X440-G2-24p-10GE4	IEC 320 C14	IEC 320 C13/C14	Min 18AWG/0.75mm ²	2x7 Terminal Block
X440-G2-48p-10GE4	IEC 320 C14	IEC 320 C13/C14	Min 16AWG/1.25mm ² (100-125VAC), Min 18AWG/.75mm ² (200-240VAC)	2x9 Terminal Block
X440-G2-24t-10GE4-DC	#6 Terminal Block	23	Min 14AWG/2.0mm ²	2x7 Terminal Block
X440-G2-48t-10GE4-DC	#6 Terminal Block	40	Min 14AWG/2.0mm ²	2x7 Terminal Block
X440-G2-24x-10GE4	IEC 320 C14	IEC 320 C13/C14	Min 18AWG/0.75mm ²	2x7 Terminal Block
X440-G2-24fx-GE4	IEC 320 C14	IEC 320 C13/C14	Min 18AWG/0.75mm ²	2x7 Terminal Block
X440-G2-12t8fx-GE4	IEC 320 C14	IEC 320 C13/C14	Min 18AWG/0.75mm ²	2x7 Terminal Block
X440-G2-24t-GE4	IEC 320 C14	IEC 320 C13/C14	Min 18AWG/0.75mm ²	2x7 Terminal Block

PoE-Plus Power Budget

Switch Model	Internal Power Supply	External RPS
X440-G2-12p-10GE4	200 W	200 W – Redundant Power Only
X440-G2-24p-10GE4	380 W	380 W – Redundant Power Only
X440-G2-48p-10GE4	740 W	1440 W – Additive Power 740 W – Redundant Power

Environmental Specifications

- EN/ETSI 300 019-2-1 v2.1.2 - Class 1.2 Storage
- EN/ETSI 300 019-2-2 v2.1.2 - Class 2.3 Transportation
- EN/ETSI 300 019-2-3 v2.1.2 - Class 3.1e Operational
- EN/ETSI 300 753 (1997-10) - Acoustic Noise
- ASTM D3580 Random Vibration Unpackaged 1.5 G

Environmental Compliance

- EU RoHS – 2011/65/EU
- EU WEEE – 2012/19/EU
- China RoHS – SJ/T 11363-2006
- Taiwan RoHS CNS 15663(2013.7)

Operating Conditions

- Temp: 0° C to 50° C (32° F to 122° F) – all models
- Temp: 0° C to 60° C (32° F to 140° F) – extended temperature range models only (16539, 16540 and 16541)
- Humidity: 10% to 95% relative humidity, non-condensing
- Altitude: 0 to 3,000 meters (9,842 feet) – All Switch Models
- Shock (half sine): 30 m/s² (3 G), 11 ms, 6 shocks
- Random vibration: 3 to 500 Hz at 1.5 G rms

Packaging and Storing Specifications

- Temp: -40° C to 70° C (-40° F to 158° F)
- Humidity: 10% to 95% relative humidity, non-condensing
- Packaged Shock (half sine): 180 m/s² (18 G), 6 ms, 600 shocks
- Packaged Vibration: 5 to 62 Hz at velocity 5 mm/s, 62 to 500 Hz at 0.2 G
- Packaged Random Vibration: 5 to 20 Hz at 1.0 ASD w/-3 dB/oct. from 20 to 200 Hz
- Packaged Drop Height: 14 drops minimum on sides and corners at 42 inches (<15 kg box)

Regulatory and Safety

North American ITE

- UL 60950-1 2nd edition A2:2014, Listed Device (U.S.)
- CSA 22.2 No. 60950-1 2nd edition 2014(Canada)
- Complies with FCC 21CFR 1040.10 (U.S. Laser Safety)
- CDRH Letter of Approval (US FDA Approval)

European ITE

- EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013 2nd Ed.
- EN 60825-1:2007 / IEC 60825-1:2007 Class 1 (Lasers Safety)
- 2014 / 35/ EU Low Voltage Directive

International ITE

- CB Report & Certificate per IEC 60950-1 : 2005+A1:2009+A2:2013 + National Differences
- AS/NZS 60950-1 (Australia /New Zealand)

EMI/EMC Standards

North American EMC for ITE

- FCC CFR 47 part 15 Class A (USA)
- ICES-003 Class A (Canada)

European EMC Standards

- EN 55032:2015 Class A
- EN 55024:2010
- EN 61000-3-2: 2014 (Harmonics)
- EN 61000-3-3: 2013 (Flicker)
- EN 300 386 v1.6.1 (EMC Telecommunications)
- 2014/30/EU EMC Directive

International EMC Certifications

- CISPR 32:2015, Class A (International Emissions)
- AS/NZS CISPR32:2015
- CISPR 24:2010 Class A (International Immunity)
- IEC 61000-4-2:2008/EN 61000-4-2:2009 Electrostatic Discharge, 8kV Contact, 15 kV Air, Criteria B
- IEC 61000-4-3:2010/EN 61000-4-3:2006 +A1:2008 +A2:2010 Radiated Immunity 10V/m, Criteria A
- IEC 61000-4-4:2012. / EN 61000-4-4:2012 Transient Burst, 1 kV, Criteria A
- IEC 61000-4-5:2014 /EN 61000-4-5:2014 Surge, 1 kV L-L, 2 kV L-G, Level 3, Criteria B
- IEC 61000-4-6:2013/EN 61000-4-6:2014 Conducted Immunity, 0.15-80 MHz, 10Vrms, 80%AM (1kHz) Criteria A
- IEC/EN 61000-4-11:2004 Power Dips & Interruptions, >30%, 25 periods, Criteria C

Country Specific

- VCCI Class A (Japan Emissions)
- ACMA RCM (Australia Emissions)
- CCC Mark
- KCC Mark, EMC Approval (Korea)

Telecom Standards

- CE 2.0 Compliant

IEEE 802.3 Media Access Standards

- IEEE 802.3ab 1000BASE-T
- IEEE 802.3z 1000BASE-X
- IEEE 802.3ae 10GBASE-X
- IEEE 802.3at PoE-Plus
- IEEE 802.3az
- IEEE 802.3u, 100Base-FX

Fan and Acoustic Noise

Switch Model	Acoustic Information	
	Bystand Sound Pressure*	Declared Sound Power (LWAD)*
X440-G2-12t-10GE4	0 dB(A) Fan Off	0 bels Fan Off
X440-G2-24t-10GE4	28.1 dB(A)	4.3 bels
X440-G2-48t-10GE4	37.9 dB(A)	5.4 bels
X440-G2-12p-10GE4	0 dB(A) Fan Off	0 bels Fan Off
X440-G2-24p-10GE4	39.4 dB(A)	5.5 bels
X440-G2-48p-10GE4	48.7 dB(A)	6.4 bels
X440-G2-24t-10GE4-DC	28.1 dB(A)	4.3 bels
X440-G2-48t-10GE4-DC	37.9 dB(A)	5.4 bels
X440-G2-24x-10GE4	26.8 dB(A)	4.0 bels
X440-G2-24fx-GE4	24.7 dB(A)	3.9 bels
X440-G2-12t8fx-GE4	23.3 dB(A)	4.0 bels
X440-G2-24t-GE4	28.1 dB(A)	4.3 bels

*- At 25°C and 50% PoE Load where applicable

External Redundant Power Supplies For Non-PoE Switches

All X440-G2 series non-PoE switches ship with one fixed internal power supply. If redundancy is required, an external RPS can be attached to the switch.

Model Number	Description
RPS-90	External redundant power supply Unit 90 Watts with cable for X440-G2-12t-10GE4 , Power cord ordered separately, order 10947 C5 to C14 Converter to utilize a C13 power cord.
STK-RPS-150PS	150 watt non-PoE redundant power supply for A, B, C, X450-G2 and X440-G2 switches, power cord ordered separately.
STK-RPS-150CH2	2-Slot modular shelf for rack-mounting 150W redundant power supplies (STK-RPS-150PS).
STK-RPS-150CH8	8-Slot modular shelf for rack-mounting 150W redundant power supplies (STK-RPS-150PS).
RPS-150XT	External redundant power supply unit 150 Watts with cable - Extended Temperature Range from 0 to +60 degrees Celsius, power cord ordered separately.
STK-RPS-1005CH3	3-Slot modular shelf for rack-mounting 150W extended temperature redundant power supplies (RPS-150XT) or 1005W PoE+ redundant power supplies (STK-RPS-1005PS).
EPS-C2	External Power System Chassis 2. Accepts up to three 750W AC PoE PSU 48V power supplies. Accepts up to 5 EPSCBL-2x7 or up to 1 EPS-CBL-2x9 cables. Ships with one EPS-CBL-2x7 cable.
EPS-CBL-2x7	External Power System Cable (1M) that connects EPS-C2 to any X440 or X450-G2 non-PoE switch for providing redundant DC power.
750W AC PSU	AC Power Supply module for EPS-C2 Chassis Redundant Power Supply, power cord ordered separately.

External Redundant Power Supplies For PoE X440-G2 Switches

All X440-G2 series PoE switches ship with fixed internal power supplies.

RPS Use Table	RPS-90	STK-RPS-150PS	RPS-150XT	EPS-C2	RPS-500P	STK-RPS-1005PS
12t	X					
24t, 24x, 48t, 24fx, 12t8fx		X	X	X	X	
12p and 24p				X	X	
48p						X

RPS Model	Redundant Power Supply Output
RPS-90	Coaxial Barrel Connector
STK-RPS-150PS	1 terminal block of 2x7 pins - provides system power and up to 150 watts of power
RPS-150XT	1 terminal block of 2x7 pins - provides system power and up to 150 watts of power
EPS-C2	1 terminal block of 2x9 pins - used for other Summit switches 5 terminal blocks of 2x7 pins - used for Summit X440-G2's
RPS-500p	1 terminal block of 2x7 pins - provides system power and up to 380 watts of IEEE802.3at power
STK-RPS-1005PS	1 terminal block of 2x9 pins - provides system power and up to 740 watts of IEEE802.3at power

RPS Model	Allowable PSU	Power Cord Input Plug/Socket	Power Cord Gauge
RPS-90	Not Applicable	IEC 320 C5/C14	Min 18AWG/0.75mm ²
STK-RPS-150PS	Not Applicable	IEC 320 C13/C14	Min 18AWG/0.75mm ²
RPS-150XT	Not Applicable	IEC 320 C13/C14	Min 18AWG/0.75mm ²
EPS-C2	Summit 750W PoE AC PSU	IEC 320 C13/C14	Min 18AWG/0.75mm ²
RPS-500p	Not Applicable	IEC 320 C13/C14	Min 18AWG/0.75mm ²
STK-RPS-1005PS	Not Applicable	IEC 320 C13/C16	Min 16AWG/1.25mm ² (100-125VAC), Min 18AWG/.75mm ² (200-240VAC)

RPS Model	Weight	Dimensions
RPS-90	0.73 lb (0.33 kg)	Height: 1.06 inches (2.69 cm) Width: 5.20 inches (13.21 cm) Depth: 2.25 inches (5.72 cm)
STK-RPS-150PS	3.85 lb (1.75 kg)	Height: 2.04 inches (5.2 cm) Width: 7.7 inches (19.6 cm) Depth: 10.1 inches (25.7 cm)
RPS-150XT	3.22 lb (1.46 kg)	Height: 1.77 inches (4.50 cm) Width: 6.07 inches (15.42 cm) Depth: 13.00 inches (33.02 cm)
EPS-C2	2.27 lb (1.03 kg)	Height: 1RU, 1.73 inches (4.4 cm) Width: 17.4 inches (44.1 cm) Depth: 15.1 inches (38.4 cm)
RPS-500p	8.06 lb (3.66 kg)	Height: 1RU, 1.73 inches (4.4 cm) Width: 17.4 inches (44.1 cm) Depth: 7.9 inches (20.1 cm)
STK-RPS-1005PS	4.63 lb (2.1kg)	Height: 1.77 inches (4.5 cm) Width: 6.07 inches (15.42 cm) Depth: 13.39 inches (34.0 cm)

Warranty

- Ltd. Lifetime with eAHR - 2
- For warranty details, visit:
<http://www.extremenetworks.com/go/warranty>

Ordering Information

Part Number	Name	Description
16530	X440-G2-12t-10GE4	X440-G2 12 10/100/1000BASE-T, 4 1GbE unpopulated SFP upgradable to 10GbE SFP+, 1 Fixed AC PSU, 1 RPS port, ExtremeXOS Edge license
16531	X440-G2-12p-10GE4	X440-G2 12 10/100/1000BASE-T POE+, 4 1GbE unpopulated SFP upgradable to 10GbE SFP+, 1 Fixed AC PSU, 1 RPS port, ExtremeXOS Edge license
16531T	X440-G2-12p-10GE4-TAA	X440-G2 12 10/100/1000BASE-T POE+, 4 1GbE unpopulated SFP upgradeable to 10GbE SFP+, 1 Fixed AC PSU, 1 RPS port, ExtremeXOS Edge license, TAA model
16532	X440-G2-24t-10GE4	X440-G2 24 10/100/1000BASE-T, 4 SFP combo, 4 1GbE unpopulated SFP upgradable to 10GbE SFP+, 1 Fixed AC PSU, 1 RPS port, ExtremeXOS Edge license

Part Number	Name	Description
16532T	X440-G2-24t-10GE4-TAA	X440-G2 24 10/100/1000BASE-T, 4 SFP combo, 4 1GbE unpopulated SFP upgradeable to 10GbE SFP+, 1 Fixed AC PSU, 1 RPS port, ExtremeXOS Edge license, TAA model
16533	X440-G2-24p-10GE4	X440-G2 24 10/100/1000BASE-T POE+, 4 SFP combo, 4 1GbE unpopulated SFP upgradeable to 10GbE SFP+, 1 Fixed AC PSU, 1 RPS port, ExtremeXOS Edge license
16533T	X440-G2-24p-10GE4-TAA	X440-G2 24 10/100/1000BASE-T POE+, 4 SFP combo, 4 1GbE unpopulated SFP upgradeable to 10GbE SFP+, 1 Fixed AC PSU, 1 RPS port, ExtremeXOS Edge license, TAA model
16534	X440-G2-48t-10GE4	X440-G2 48 10/100/1000BASE-T, 4 SFP combo, 4 1GbE unpopulated SFP upgradeable to 10GbE SFP+ (2 combo/2 non-combo), 2 1GbE copper combo upgradeable to 10GbE, 1 Fixed AC PSU, 1 RPS port, ExtremeXOS Edge license
16535	X440-G2-48p-10GE4	X440-G2 48 10/100/1000BASE-T POE+, 4 SFP combo, 4 1GbE unpopulated SFP upgradeable to 10GbE SFP+ (2 combo/2 non-combo), 2 1GbE copper combo upgradeable to 10GbE, 1 Fixed AC PSU, 1 RPS port, ExtremeXOS Edge license
16535T	X440-G2-48p-10GE4-TAA	X440-G2 48 10/100/1000BASE-T POE+, 4 SFP combo, 4 1GbE unpopulated SFP upgradeable to 10GbE SFP+ (2 combo/2 non-combo), 2 1GbE copper combo upgradeable to 10GbE, 1 Fixed AC PSU, 1 RPS port, ExtremeXOS, TAA model
16536	X440-G2-24t-10GE4-DC	X440-G2 24 10/100/1000BASE-T, 4 SFP combo, 4 1GbE unpopulated SFP upgradeable to 10GbE SFP+, 1 Fixed DC PSU, 1 RPS port, ExtremeXOS Edge license
16537	X440-G2-48t-10GE4-DC	X440-G2 48 10/100/1000BASE-T, 4 SFP combo, 4 1GbE unpopulated SFP upgradeable to 10GbE SFP+ (2 combo/2 non-combo), 2 1GbE copper combo upgradeable to 10GbE, 1 Fixed DC PSU, 1 RPS port, ExtremeXOS Edge license
16538	X440-G2-24x-10GE4	X440-G2 24 unpopulated 1000BASE-X SFP (4 combo), 4 10/100/1000 combo, 4 1GbE unpopulated SFP upgradeable to 10GbE SFP+, 1 Fixed AC PSU, 1 RPS port, ExtremeXOS Edge license
16538T	X440-G2-24x-10GE4-TAA	X440-G2 24 unpopulated 1000BASE-X SFP (4 combo), 4 10/100/1000 combo, 4 1GbE unpopulated SFP, upgradeable to 10GbE SFP+, 1 Fixed AC PSU, 1 RPS port, ExtremeXOS Edge license, TAA model
16539	X440-G2-24fx-GE4	X440-G2 24 fixed 100BASE-FX LC connectors, 4 1GBASE-X unpopulated SFP, 1 Fixed AC PSU, 1 RPS port, ExtremeXOS Edge license, 0°C to 60°C operation
16540	X440-G2-12t8fx-GE4	X440-G2 12 10/100/1000BASE-T plus 8 fixed 100BASE-FX LC connectors, 4 1GBASE-X unpopulated SFP, 1 Fixed AC PSU, 1 RPS port, ExtremeXOS Edge license, 0°C to 60°C operation
16541	X440-G2-24t-GE4	X440-G2 24 fixed 10/100/1000BASE-TX, 4 1GBASE-X unpopulated SFP, 1 Fixed AC PSU, 1 RPS port, ExtremeXOS Edge license, 0°C to 60°C operation
16521	X440 Adv. Edge License	ExtremeXOS Advanced Edge License for X440/X440-G2 series switches
16522	X440 OpenFlow Feature Pack	ExtremeXOS SDN - OpenFlow Feature Pack for X440/X440-G2 series switches
16523	X440 Multimedia(AVB) Feature Pack	ExtremeXOS Multimedia Service (Audio Video Bridging) Feature Pack for X440/X440-G2 series switches
16542	Dual 10GbE Upgrade License	License that converts the two non-stack 1GbE SFP ports to be 10GbE SFP+
16543	Quad 10GbE Upgrade License	License that converts four 1GbE SFP ports to be 10GbE SFP+
16546	Quad 10GbE Lic from Dual 10GbE Lic	Software license that upgrades an already licensed X440-G2 Dual 10GbE switch to a Quad 10GbE switch
10301	10GBASE-SR SFP+	10GBASE-SR SFP+, 850nm, LC Connector, transmission length of up to 300m on MMF
10302	10GBASE-LR SFP+	10GBASE-LR SFP+, 1310nm, LC Connector, transmission length of up to 10km on SMF
10309	10GBASE-ER SFP+	10GBASE-ER SFP+, 1550nm, LC connector, transmission length of up to 40km on SMF
10303	SFP+ LRM Module	10 Gigabit Ethernet SFP+ module, 1310nm, legacy MMF 220m link, LC connector

Part Number	Name	Description
10948	RPS-90	External Redundant Power Supply Unit 90 Watts with cable , Power cord ordered separately
10947	C5 to C14 Converter	Power dongle for converting an IEC C5 plug to IEC C14 plug - enables the use of to utilize a C13 power cord
STK-RPS-150PS	150W Non-PoE RPS	150 watt non-PoE redundant power supply for A, B, C and X450-G2 switches
STK-RPS-150CH2	2-Slot Modular Shelf	2-Slot Modular Shelf for rack mounting up to two150 watt (STK-RPS-150PS) external redundant power supplies
STK-RPS-150CH8	8-Slot Modular Shelf	8-Slot Modular Shelf for rack mounting up to eight 150 watt (STK-RPS-150PS) external redundant power supplies
10932	RPS-150 XT	External Redundant Power Supply Unit 150 Watts with cable - Extended Temperature Range from 0 to +60 degrees Celsius, Power cord ordered separately
10923	RPS-500p	External PoE+ Redundant Power Supply Unit 500 Watts with cable, Power cord ordered separately
STK-RPS-1005PS	1005 W RPS	1005 watt 802.3at PoE external redundant power supply for C5 PoE and X440-48p switches
STK-RPS-1005CH3	3-Slot Modular Shelf	3-Slot Modular Shelf for rack mounting up to three of any combination of extended temperature 150 watt (10932 - RPS-150 XT) or STK-RPS-1005PS external redundant power supplies
10936	EPS-C2	External Power System Chassis 2. Accepts up to three 750W AC PoE PSU 48V power supplies. Accepts up to 5 EPS-CBL-2x7 or up to 1 EPS-CBL-2x9 cables
10939	EPS-CBL-2x7	External Power System Cable (1M with 2x7 pin) that connects EPS to any X440 or X450-G2 for providing redundant power
10931	750W AC PSU	AC Power Supply module for EPS-C2 Chassis Redundant Power Supply
10051H	1000BASE-SX SFP, Hi	1000BASE-SX SFP, MMF 220 & 550 meters, LC connector, Industrial Temp
10052H	1000BASE-LX SFP, Hi	1000BASE-LX SFP, MMF 220 & 550 meters, SMF 10km, LC connector, Industrial Temp
10053H	1000BASE-ZX SFP, Hi	1000BASE-ZX SFP, SMF 70km, LC connector, Industrial Temp
10056H	1000BASE-BX-D BiDi SFP, Hi	1000BASE-BX-D SFP, 1490-nm TX/1310-nm RX wavelength, Industrial Temp
10057H	1000BASE-BX-U BiDi SFP, Hi	1000BASE-BX-U SFP, 1310-nm TX/1490-nm RX wavelength, Industrial Temp
10060	100FX/1000LX SFP2	100FX/1000LX SFP, SMF, LC Connector (Requires MCP and 6dB Attenuator for 100FX-MMF Operation) ²
10070H	10/100/1000BASE-T SFP, Hi ²	10/100/1000BASE-T, SFP, CAT 5 cable 100m, RJ-45 Connector, Industrial Temp ²
10071H	1000BASE-SX SFP 10 Pack, Hi	1000BASE-SX SFP 10 Pack, Industrial Temp
10072H	1000BASE-LX SFP 10 Pack, Hi	1000BASE-LX SFP 10 Pack, Industrial Temp
MGBIC-BX120-D	1000BASE-BX-D BiDi SFP 120Km	1 Gb, 1000Base-BX120-D Single Fiber SM, Bidirectional, 1590nm Tx / 1490nm Rx, 120 Km, Simplex LC SFP (must be paired with MGBIC-BX120-U), -40°C to +60°C
MGBIC-BX120-U	1000BASE-BX-U BiDi SFP 120Km	1 Gb, 1000Base-BX120-U Single Fiber SM, Bidirectional, 1490nm Tx / 1590nm Rx, 120 Km, Simplex LC SFP (must be paired with MGBIC-BX120-D), -40°C to +60°C
10063	100FX SFP ¹	100Mb, 100BASE-FX, MMF 2Km, LC ¹
10067	100BASE-FX SFP ¹	100BASE-FX SFP module, MMF 2km link, LC-connector for Fast Ethernet SFP Port ¹
10304	10GBASE-CR SFP+ 1m	10GBASE-CR SFP+ pre-terminated twin-ax copper cable with link lengths of 1m
10305	10GBASE-CR SFP+ 3m	10GBASE-CR SFP+ pre-terminated twin-ax copper cable with link lengths of 3m
10306	10GBASE-CR SFP+ 5m	10GBASE-CR SFP+ pre-terminated twin-ax copper cable with link lengths of 5m
10307	10GBASE-CR SFP+ 10m3	10GBASE-CR SFP+ pre-terminated twin-ax copper cable with link lengths of 10m*
10325	DWDM SFP+	10 Gigabit Ethernet SFP+ Tunable DWDM module, SMF 80km, LC connector
10338	10Gb SFP+ 10GBASE-T ⁴	10Gb SFP+, 10GBASE-T RJ45, 30m with Cat6a ⁴

Part Number	Name	Description
10GB-ZR-SFPP	10GB 80KM SFP+	10Gb, 10GBASE-ZR, SM, 1550nm, 80Km, LC SFP+
10GB-BX40-D	10 GB, SINGLE FIBER SM, -D 40 KM	10Gb, Single Fiber SM, Bidirectional, 1330nm Tx / 1270nm RX, 40Km, Simplex LC SFP+ (must be paired with 10GB-BX40-U)
10GB-BX40-U	10 GB, SINGLE FIBER SM, -U 40 KM	10Gb, Single Fiber SM, Bidirectional, 1270nm Tx / 1330nm RX, 10Km, Simplex LC SFP+ (must be paired with 10GB-BX40-D)
10GB-BX10-D	10 GB, SINGLE FIBER SM, -D 10 KM	10Gb, Single Fiber SM, Bidirectional, 1330nm Tx / 1330nm RX, 40Km, Simplex LC SFP+ (must be paired with 10GB-BX10-U)
10GB-BX10-U	10 GB, SINGLE FIBER SM, -U 10 KM	10Gb, Single Fiber SM, Bidirectional, 1270nm Tx / 1330nm RX, 10Km, Simplex LC SFP+ (must be paired with 10GB-BX10-D)
10GB-F10-SFPP	10 GB, ACTIVE OPTICAL DAC, 10 M	10Gb, Active optical direct attach cable with 2 integrated SFP+ transceivers, 10m
10GB-F20-SFPP	10 GB, ACTIVE OPTICAL DAC, 20 M	10Gb, Active optical direct attach cable with 2 integrated SFP+ transceivers, 20m
MGBIC-BX40-D	1000BASE-BX40-D BIDIRECTIONAL SFP	1Gb, 1000Base-BX40-D Single Fiber SM, Bidirectional, 1490nm Tx / 1310nm RX, 40Km, Simplex LC SFP (must be paired with MGBIC-BX40-U), -40°C to +60°C
MGBIC-BX40-U	1000BASE-BX40-U BIDIRECTIONAL SFP	1Gb, 1000Base-BX40-U Single Fiber SM, Bidirectional, 1310nm Tx / 1490nm RX, 40Km, Simplex LC SFP (must be paired with MGBIC-BX40-D), -40°C to +60°C
MGBIC-BX10-D	1000BASE-BX-D SFP - 10KM	1Gb, 1000Base-BX10-D Single Fiber SM, Bidirectional, 1490nm Tx / 1310nm RX, 10Km, Simplex LC SFP (must be paired with MGBIC-BX10-U)
MGBIC-BX10-U	1000BASE-BX-U SFP - 10KM	1Gb, 1000Base-BX10-U Single Fiber SM, Bidirectional, 1310nm Tx / 1490nm RX, 10Km, Simplex LC SFP (must be paired with MGBIC-BX10-D)
I-MGBIC-LC03	Industrial 1000Base-LX 1310nm MMF Transceiver	-40°C to +60°C, 1Gb, 1000Base-LX, MM, 1310 nm, 2 km with 62.5 MMF, 1 km with 50 MMF, LC SFP
I-MGBIC-GSX	Industrial 1000Base-SX 850nm Transceiver	-40°C to +60°C, 1Gb, 1000Base-SX, IEEE 802.3 MM, 850nm Short Wave Length, 220/550m, LC SFP
I-MGBIC-GLX	Industrial 1000Base-LX 1310nm SM Transceiver	-40°C to +60°C, 1Gb, 1000Base-LX, MM - 550m, SM - 10 km, 1310 nm Long Wave Length, LC SFP, LC SFP

¹ - Supported in 24 SFP ports in 16538, not supported on SFP combo ports or SFP/SFP+ uplink ports.

² - Supported in 24 SFP ports in 16538, not supported on SFP combo ports, 1Gb Mode Only on SFP/SFP+ uplink port.

³ - Supported on 48 port 10GbE ports only ExtremeCloud Management - 16530, 16531, 16532, 16533, 16534 and 16535 switches are enabled for use with ExtremeCloud. For details and ordering part numbers for ExtremeCloud Management, see the ExtremeCloud datasheet.

⁴ Supported configuration is to populate every other SFP+ port in system, with a maximum of half the 10Gb SFP+ ports configured with 10GBASE-T transceivers. An adjacent SFP+ port should remain unused for every 10GBASE-T SFP+ installed

SRX300 Line of Services Gateways for the Branch



Product Overview

The SRX300 line of services gateways combines security, routing, switching, and WAN interfaces with next-generation firewall and advanced threat mitigation capabilities for cost-effective, secure connectivity across distributed enterprise locations. By consolidating fast, highly available switching, routing, security, and next-generation firewall capabilities in a single device, enterprises can remove network complexity, protect and prioritize their resources, and improve user and application experience while lowering total cost of ownership (TCO).

Product Description

Juniper Networks® SRX300 line of services gateways delivers a next-generation networking and security solution that supports the changing needs of cloud-enabled enterprise networks. Whether rolling out new services and applications across locations, connecting to the cloud, or trying to achieve operational efficiency, the SRX300 line helps organizations realize their business objectives while providing scalable, easy to manage, secure connectivity and advanced threat mitigation capabilities. Next-generation firewall and unified threat management (UTM) capabilities also make it easier to detect and proactively mitigate threats to improve the user and application experience.

The SRX300 line consists of four models:

- **SRX300:** Securing small branch or retail offices, the SRX300 Services Gateway consolidates security, routing, switching, and WAN connectivity in a small desktop device. The SRX300 supports up to 1 Gbps firewall and 300 Mbps IPsec VPN in a single, consolidated, cost-effective networking and security platform.
- **SRX320:** Securely connecting small distributed enterprise branch offices, the SRX320 Services Gateway consolidates security, routing, switching, and WAN connectivity in a small desktop device. The SRX320 supports up to 1 Gbps firewall and 300 Mbps IPsec VPN in a single, consolidated, cost-effective networking and security platform.
- **SRX340:** Securely connecting midsize distributed enterprise branch offices, the SRX340 Services Gateway consolidates security, routing, switching, and WAN connectivity in a 1 U form factor. The SRX340 supports up to 3 Gbps firewall and 600 Mbps IPsec VPN in a single, consolidated, cost-effective networking and security platform.
- **SRX345:** Best suited for midsize to large distributed enterprise branch offices, the SRX345 Services Gateway consolidates security, routing, switching, and WAN connectivity in a 1 U form factor. The SRX345 supports up to 5 Gbps firewall and 800 Mbps IPsec VPN in a single, consolidated, cost-effective networking and security platform.

SRX300 Highlights

The SRX300 line of services gateways consists of secure routers that bring high performance and proven deployment capabilities to enterprises that need to build a worldwide network of thousands of remote sites. Ethernet, serial, T1/E1, ADSL2/2+, VDSL2, and 3G/4G LTE wireless are all available options for WAN or Internet connectivity to link sites. Industry best, high-performance IPsec VPN solutions provide comprehensive encryption and authentication capabilities to secure intersite communications. Multiple form factors with Ethernet switching support on native Gigabit Ethernet ports allow cost-effective choices for mission-critical deployments. Juniper Networks Junos® automation and scripting capabilities and Junos Space Security Director reduce operational complexity and simplify the provisioning of new sites.



The SRX300 line of devices recognizes more than 3,500 Layer 3-7 applications, including Web 2.0 and evasive peer-to-peer (P2P) applications like Skype, torrents, and others. Correlating application information with user contextual information, the SRX300 line can generate bandwidth usage reports, enforce access control policies, prioritize and rate-limit traffic going out of WAN interfaces, and proactively secure remote sites. This optimizes resources in the branch office and improves the application and user experience.

For the perimeter, the SRX300 line offers a comprehensive suite of application security services, threat defenses, and intelligence services. The services consist of intrusion prevention system (IPS), application security user role-based firewall controls, and on-box and cloud-based antivirus, anti-spam, and enhanced Web filtering, protecting networks from the latest content-borne threats. Integrated threat intelligence via Juniper Networks Spotlight Secure offers adaptive threat protection

against Command and Control (C&C)-related botnets and policy enforcement based on GeoIP. Customers can also leverage their own custom and third-party feeds for protection from advanced malware and other threats. Integrating the Juniper Networks Sky Advanced Threat Protection solution, the SRX300 line detects and enforces automated protection against known malware and zero-day threats with a very high degree of accuracy.

The SRX300 line enables agile SecOps through automation capabilities that support Zero Touch Deployment, Python scripts for orchestration, and event scripting for operational management.

SRX300 services gateways run Juniper Networks Junos operating system, a proven, carrier-hardened network OS that powers the top 100 service provider networks around the world. The rigorously tested, carrier-class, rich routing features such as IPv4/IPv6, OSPF, BGP, and multicast have been proven in over 15 years of worldwide deployments.

Features and Benefits

Business Requirement	Feature/Solution	SRX300 Advantages
High performance	Up to 5 Gbps of routing and firewall performance	<ul style="list-style-type: none"> Best suited for small, medium and large branch office deployments Addresses future needs for scale and feature capacity
Business continuity	Stateful high availability (HA), IP monitoring	<ul style="list-style-type: none"> Uses stateful HA to synchronize configuration and firewall sessions Supports multiple WAN interface with dial-on-demand backup Route/link failover based on real-time link performance
End-user experience	App visibility and control	<ul style="list-style-type: none"> Detects 3,500+ Layer 3-7 applications, including Web 2.0 Controls and prioritizes traffic based on application and use role Inspects and detects applications inside the SSL encrypted traffic
Highly secure	IPsec VPN, Media Access Control Security (MACsec) ¹	<ul style="list-style-type: none"> Creates secure, reliable, and fast overlay link over public internet Employs anti-counterfeit features to protect from unauthorized hardware spares High-performance CPU with built-in hardware assist IPsec acceleration TPM-based protection of device secrets such as passwords and certificates
Threat protection	IPS, antivirus, anti-spam, Spotlight Secure, Sky Advanced Threat Prevention ²	<ul style="list-style-type: none"> Enables zone-based stateful firewall by default Protects from malware and attacks with IPS and antivirus Integrates open threat intelligence platform with third-party feeds Defends against zero-day attacks
Easy to manage and scale	On-box GUI, Security Director	<ul style="list-style-type: none"> Includes centralized management for auto-provisioning, firewall policy management, Network Address Translation (NAT), and IPsec VPN deployments Includes simple easy-to-use on-box GUI for local management
Minimize TCO	Junos OS	<ul style="list-style-type: none"> Integrates routing, switching, and security in a single device Reduces operation expense with Junos automation capabilities



SRX300



SRX320



SRX340



SRX345

¹MACsec for LAN/WAN links available in 15.1X49-D100 and later releases.

²SSL forward proxy and Sky ATP are supported on SRX340 and higher platforms.

SRX300 Specifications

Software Specifications

Routing Protocols

- IPv4, IPv6, ISO, Connectionless Network Service (CLNS)
- Static routes
- RIP v1/v2
- OSPF/OSPF v3
- BGP with Route Reflector
- IS-IS
- Multicast: Internet Group Management Protocol (IGMP) v1/v2, Protocol Independent Multicast (PIM) sparse mode (SM)/dense mode (DM)/source-specific multicast (SSM), Session Description Protocol (SDP), Distance Vector Multicast Routing Protocol (DVMRP), Multicast Source Discovery Protocol (MSDP), Reverse Path Forwarding (RPF)
- Encapsulation: VLAN, Point-to-Point Protocol (PPP), Frame Relay, High-Level Data Link Control (HDLC), serial, Multilink Point-to-Point Protocol (MLPPP), Multilink Frame Relay (MLFR), and Point-to-Point Protocol over Ethernet (PPPoE)
- Virtual routers
- Policy-based routing, source-based routing
- Equal-cost multipath (ECMP)

QoS Features

- Support for 802.1p, DiffServ code point (DSCP), EXP
- Classification based on VLAN, data-link connection identifier (DLCI), interface, bundles, or multifield filters
- Marking, policing, and shaping
- Classification and scheduling
- Weighted random early detection (WRED)
- Guaranteed and maximum bandwidth
- Ingress traffic policing
- Virtual channels
- Hierarchical shaping and policing

Switching Features

- ASIC-based Layer 2 Forwarding
- MAC address learning
- VLAN addressing and integrated routing and bridging (IRB) support
- Link aggregation and LACP
- LLDP and LLDP-MED
- STP, RSTP, MSTP
- MVRP
- 802.1X authentication

Firewall Services

- Stateful and stateless firewall
- Zone-based firewall
- Screens and distributed denial of service (DDoS) protection
- Protection from protocol and traffic anomaly
- Integration with Pulse Unified Access Control (UAC)
- Integration with Aruba Clear Pass Policy Manager
- User role-based firewall
- SSL Inspection (Forward-proxy)²

Network Address Translation (NAT)

- Source NAT with Port Address Translation (PAT)
- Bidirectional 1:1 static NAT
- Destination NAT with PAT
- Persistent NAT
- IPv6 address translation

VPN Features

- Tunnels: Generic routing encapsulation (GRE)³, IP-IP³, IPsec
- Site-site IPsec VPN, auto VPN, group VPN
- IPsec crypto algorithms: Data Encryption Standard (DES), triple DES (3DES), Advanced Encryption Standard (AES-256), AES-GCM
- IPsec authentication algorithms: MD5, SHA-1, SHA-128, SHA-256
- Pre-shared key and public key infrastructure (PKI) (X.509)
- Perfect forward secrecy, anti-reply
- IPv4 and IPv6 IPsec VPN
- Multi-proxy ID for site-site VPN
- Internet Key Exchange (IKEv1, IKEv2), NAT-T
- Virtual router and quality-of-service (QoS) aware
- Standard-based dead peer detection (DPD) support
- VPN monitoring

Network Services

- Dynamic Host Configuration Protocol (DHCP) client/server/relay
- Domain Name System (DNS) proxy, dynamic DNS (DDNS)
- Juniper real-time performance monitoring (RPM) and IP-monitoring
- Juniper flow monitoring (J-Flow)³

High Availability Features

- Virtual Router Redundancy Protocol (VRRP)³
- Stateful high availability
 - Dual box clustering
 - Active/passive
 - Active/active
 - Configuration synchronization
 - Firewall session synchronization
 - Device/link detection
 - In-Band Cluster Upgrade (ICU)
- Dial on-demand backup interfaces
- IP monitoring with route and interface failover

Management, Automation, Logging, and Reporting

- SSH, Telnet, SNMP
- Smart image download
- Juniper CLI and Web UI
- Junos Space and Security Director
- Python
- Junos OS event, commit, and OP script
- Application and bandwidth usage reporting
- Auto installation
- Debug and troubleshooting tools
- Zero-Touch Provisioning with Contrail Service Orchestration

³GRE, IP-IP, J-Flow monitoring, and VRRP are not supported in stateful high-availability mode.

Advanced Routing Services

- Packet mode
- MPLS (RSVP, LDP)
- Circuit cross-connect (CCC), translational cross-connect (TCC)
- L2/L3 MPLS VPN, pseudowires
- Virtual private LAN service (VPLS), next-generation multicast VPN (NG-MVPN)
- MPLS traffic engineering and MPLS fast reroute

Application Security Services⁴

- Application visibility and control
- Application-based firewall
- Application QoS
- Application-based advanced policy-based routing

Threat Defense and Intelligence Services⁵

- Intrusion prevention
- Antivirus
- Antispam
- Category/reputation-based URL filtering
- Spotlight Secure threat intelligence
- Protection from botnets (command and control)
- Adaptive enforcement based on GeoIP
- Sky Advanced Threat Prevention to detect and block zero-day attacks⁶

Hardware Specifications

Specification	SRX300	SRX320	SRX340	SRX345
Connectivity				
Total onboard ports	8x1GbE	8x1GbE	16x1GbE	16x1GbE
Onboard RJ-45 ports	6x1GbE	6x1GbE	8x1GbE	8x1GbE
Onboard small form-factor pluggable (SFP) transceiver ports	2x1GbE	2x1GbE	8x1GbE	8x1GbE
MACsec-capable ports	2x1GbE	2x1GbE	16x1GbE	16x1GbE
Out-of-band (OOB) management ports	0	0	1x1GbE	1x1GbE
Mini PIM (WAN) slots	0	2	4	4
Console (RJ-45 + miniUSB)	1	1	1	1
USB 3.0 ports (type A)	1	1	1	1
Optional PoE+ ports	N/A	6 ⁷	0	0
Memory and Storage				
System memory (RAM)	4 GB	4 GB	4 GB	4 GB
Storage (flash)	8 GB	8 GB	8 GB	8 GB
SSD slots	0	0	1	1
Dimensions and Power				
Form factor	Desktop	Desktop	1 U	1 U
Size (WxHxD)	12.63 x 1.37 x 7.52 in. (32.08 x 3.47 x 19.10 cm)	11.81 x 1.73 x 7.52 in. (29.99 x 4.39 x 19.10 cm)	17.36 x 1.72 x 14.57 in. (44.09 x 4.36 x 37.01 cm)	17.36 x 1.72 x 14.57 in. (44.09 x 4.36 x 37.01 cm) / 17.36 x 1.72 x 18.7 in. (44.09 x 4.36 x 47.5 cm) ⁸
Weight (device and PSU)	4.38 lb (1.98 kg)	3.28 lb (1.51 kg) ⁹ / 3.4 lb (1.55 kg) ¹⁰	10.80 lb (4.90 kg)	10.80 lb (4.90 kg)
Redundant PSU	No	No	No	Yes
Power supply	AC (external)	AC (external)	AC (internal)	AC (internal)
Maximum PoE power	N/A	180 W ¹⁰	N/A	N/A
Average power consumption	15.4 W	27 W ⁹ /112 W ¹⁰	122 W	122 W
Average heat dissipation	85 BTU/h	157 BTU/h ⁹ /755 BTU/h ¹⁰	420 BTU/h	420 BTU/h
Maximum current consumption	0.254 A	0.473 A ⁹ /2.07 A ¹⁰	1.364 A	1.364 A
Acoustic noise level	0dB (fanless)	37 dBA ⁹ /40 dBA ¹⁰	45.5 dBA	45.5 dBA
Airflow/cooling	Fanless	Front to back	Front to back	Front to back

⁴ Available as part of Junos Software Enhanced (JSE) software package or advanced security subscription licenses.⁵ Offered as advanced security services subscription licenses.⁶ Sky ATP is supported on SRX340 and higher platforms.⁷ PoE ports on SRX320 available as a separate SKU: SRX320-POE.⁸ SRX345 with dual AC PSU model.⁹ SRX320 non PoE model.¹⁰ SRX320-POE with 6 ports PoE+ model.

Specification	SRX300	SRX320	SRX340	SRX345
Environmental, Compliance, and Safety Certification				
Operational temperature			32° to 104° F (0° to 40° C)	
Nonoperational temperature			4° to 158° F (-20° to 70° C)	
Operating humidity			10% to 90% noncondensing	
Nonoperating humidity			5% to 95% noncondensing	
Meantime between failures (MTBF)	44.5 years	32.5 years ⁹ / 26 years ¹⁰	27 years	27.4 years
FCC classification	Class A	Class A	Class A	Class A
RoHS compliance	RoHS 2	RoHS 2	RoHS 2	RoHS 2
Common Criteria certification		NDPP, VPNEP, FWEP, IPSEP (based on Junos 15.1X49-D60)		

Performance and Scale

Parameter	SRX300	SRX320	SRX340	SRX345
Routing with packet mode (64 B packet size) in Kpps ¹¹	300	300	550	750
Routing with packet mode (IMIX packet size) in Mbps ¹¹	800	800	1,600	2,300
Routing with packet mode (1,518 B packet size) in Mbps ¹¹	1,500	1,500	3,000	5,500
Stateful firewall (64 B packet size) in Kpps ¹¹	200	200	350	550
Stateful firewall (IMIX packet size) in Mbps ¹¹	500	500	1,100	1,700
Stateful firewall (1,518 B packet size) in Mbps ¹¹	1,000	1,000	3,000	5,000
IPsec VPN (IMIX packet size) in Mbps ¹¹	100	100	200	300
IPsec VPN (1,400 B packet size) in Mbps ¹¹	300	300	600	800
Application visibility and control in Mbps ¹²	500	500	1,000	1,700
Recommended IPS in Mbps ¹²	200	200	400	600
Next-generation firewall in Mbps ¹²	100	100	200	300
Route table size (RIB/FIB) (IPv4 or IPv6)	256,000/256,000	256,000/256,000	1 million/600,000 ¹³	1 million/600,000 ¹³
Maximum concurrent sessions (IPv4 or IPv6)	64,000	64,000	256,000	375,000
Maximum security policies	1,000	1,000	2,000	4,000
Connections per second	5,000	5,000	10,000	15,000
NAT rules	1,000	1,000	2,000	2,000
MAC table size	15,000	15,000	15,000	15,000
IPsec VPN tunnels	256	256	1,024	2,048
Number of remote access uses	25	50	150	250
GRE tunnels	256	256	512	1,024
Maximum number of security zones	16	16	64	64
Maximum number of virtual routers	32	32	64	128
Maximum number of VLANs	1,000	1,000	2,000	3,000
ApplD sessions	16,000	16,000	64,000	64,000
IPS sessions	16,000	16,000	64,000	64,000
URLF sessions	16,000	16,000	64,000	64,000

¹¹Throughput numbers based on UDP packets and RFC2544 test methodology.

¹²Throughput numbers based on HTTP traffic with 44 KB transaction size.

¹³Route scaling numbers are with enhanced route-scale features turned on.

WAN Interface Support Matrix

WAN Interface	SRX300	SRX320	SRX340	SRX345
1 port T1/E1 MPIM (SRX-MP-1T1E1-R)	No	Yes	Yes	Yes
1 port VDSL2 Annex A/M MPIM (SRX-MP-1VDSL2-R)	No	Yes	Yes	Yes
1 port serial MPIM (SRX-MP-1SERIAL-R)	No	Yes	Yes	Yes
4G / LTE MPIM (SRX-MP-LTE-AA & SRX-MP-LTE-AE)	No	Yes	Yes	Yes

Ordering Information

The SRX300 line offers a number of flexible ordering options. Customers can choose the Junos software package for each SRX300 line platform purchased based on their needs. Two Junos software packages are available with the SRX300 line hardware: Junos Software Base (JSB/JB) and Junos Software Enhanced (JSE/JE). All routing, firewall, IPSec, and advanced networking services are included in the JSB/JB package. The JSE/JE package includes all JSB capabilities, plus application security services (application identification, application firewall, application QoS, and application routing). Advanced security services intrusion prevention, content security, and Sky Advanced Threat Protection are offered as annual subscription-based services with any of the Junos software packages.

	SRXnnn-SYS-JB	SRXnnn-SYS-JE
Hardware	Included	Included
Management (CLI, JWEB, SNMP, Telnet, SSH)	■	■
Ethernet switching (L2 Forwarding, IRB, LACP etc)	■	■
L2 Transparent, Secure Wire	■	■
Routing (RIP, OSPF, BGP, Virtual router)	■	■
Multicast (IGMP, PIM, SSDP, DMVRP)	■	■
Packet Mode	■	■
Overlay (GRE, IP-IP)	■	■
Network Services (J-Flow, DHCP, QOS, BFD)	■	■
Stateful Firewall, Screens, ALGs	■	■
NAT (static, SNAT, DNAT)	■	■
IPSec VPN (Site-Site VPN, Auto VPN, Group VPN)	■	■
Firewall policy enforcement (UAC, Aruba CPPM)	■	■
Remote Access VPN (2 free licenses)	L	L
Chassis Cluster, VRRP, ISSU / ICU	■	■
Automation (Junos scripting, auto-installation)	■	■
MPLS, LDP, RSVP, L3 VPN, pseudo-wires, VPLS	■	■
Application Security (AppID, AppFW, AppQOS, AppRoute)		■

L = Per-user license-based; two free user licenses included

Base System Model Numbers

Product Number	Description
SRX300-SYS-JB	SRX300 Services Gateway includes hardware (8GbE, 4G RAM, 8G Flash, power adapter and cable) and Junos Software Base (firewall, NAT, IPSec, routing, MPLS and switching). RMK not included.
SRX300-SYS-JE	SRX300 Services Gateway includes hardware (8GbE, 4G RAM, 8G Flash, power adapter and cable) and Junos Software Enhanced (firewall, NAT, IPSec, routing, MPLS, switching and application security). RMK not included.
SRX320-SYS-JB	SRX320 Services Gateway includes hardware (8GbE, 2x MPIM slots, 4G RAM, 8G Flash, power adapter and cable) and Junos Software Base (firewall, NAT, IPSec, routing, MPLS and switching). RMK not included.
SRX320-SYS-JE	SRX320 Services Gateway includes hardware (8GbE, 2x MPIM slots, 4G RAM, 8G Flash, power adapter and cable) and Junos Software Enhanced (firewall, NAT, IPSec, routing, MPLS, switching and application security). RMK not included.
SRX320-SYS-JB-P	SRX320 Services Gateway includes hardware (8GbE, 6-port POE+, 2x MPIM slots, 4G RAM, 8G Flash, power adapter and cable) and Junos Software Base (firewall, NAT, IPSec, routing, MPLS and switching). RMK not included.
SRX320-SYS-JE-P	SRX320 Services Gateway includes hardware (8GbE, 6-port POE+, 2x MPIM slots, 4G RAM, 8G Flash, power adapter and cable) and Junos Software Enhanced (firewall, NAT, IPSec, routing, MPLS, switching and application security). RMK not included.
SRX340-SYS-JB	SRX340 Services Gateway includes hardware (16GbE, 4x MPIM slots, 4G RAM, 8G Flash, power supply, cable and RMK) and Junos Software Base (firewall, NAT, IPSec, routing, MPLS and switching)
SRX340-SYS-JE	SRX340 Services Gateway includes hardware (16GbE, 4x MPIM slots, 4G RAM, 8G Flash, power supply, cable and RMK) and Junos Software Enhanced (firewall, NAT, IPSec, routing, MPLS, switching and application security)
SRX345-SYS-JB	SRX345 Services Gateway includes hardware (16GbE, 4x MPIM slots, 4G RAM, 8G Flash, power supply, cable and RMK) and Junos Software Base (firewall, NAT, IPSec, routing, MPLS and switching)
SRX345-SYS-JE	SRX345 Services Gateway includes hardware (16GbE, 4x MPIM slots, 4G RAM, 8G Flash, power supply, cable and RMK) and Junos Software Enhanced (firewall, NAT, IPSec, routing, MPLS, switching and application security)
SRX345-SYS-JB-2AC	SRX345 Services Gateway includes hardware (16GbE, 4x MPIM slots, 4G RAM, 8G Flash, dual AC power supply, cable and RMK) and Junos Software Base (firewall, NAT, IPSec, routing, MPLS and switching)
SRX345-SYS-JE-2AC	SRX345 Services Gateway includes hardware (16GbE, 4x MPIM slots, 4G RAM, 8G Flash, dual AC power supply, cable and RMK) and Junos Software Enhanced (firewall, NAT, IPSec, routing, MPLS, switching and application security)

Remote Access VPN (Dynamic VPN) Licenses

Product Number	Description
SRX-RAC-5-LTU	Dynamic VPN service: 5 simultaneous Access Manager users
SRX-RAC-10-LTU	Dynamic VPN service: 10 simultaneous Access Manager users
SRX-RAC-25-LTU	Dynamic VPN service: 25 simultaneous Access Manager users
SRX-RAC-50-LTU	Dynamic VPN service: 50 simultaneous Access Manager users
SRX-RAC-100-LTU	Dynamic VPN service: 100 simultaneous Access Manager users
SRX-RAC-150-LTU	Dynamic VPN service: 150 simultaneous Access Manager users
SRX-RAC-250-LTU	Dynamic VPN service: 250 simultaneous Access Manager users
SRX-RAC-500-LTU	Dynamic VPN service: 500 simultaneous Access Manager users

Interfaces Modules

Product Number	Description
SRX-MP-1T1E1-R	1 port T1E1, MPIM form factor supported on SRX320, SRX340, SRX345 and SRX550M. ROHS complaint
SRX-MP-1VDSL2-R	1 port VDSL2 (backward compatible with ADSL / ADSL2+), MPIM form factor supported on SRX320, SRX340, SRX345 and SRX550M. ROHS complaint
SRX-MP-1SERIAL-R	1 port Synchronous Serial, MPIM form factor supported on SRX320, SRX340, SRX345 and SRX550M. ROHS complaint
SRX-MP-LTE-AA	4G / LTE MPIM support 1, 3, 5, 7-8, 18-19, 21, 28, 38-41 LTE bands (for Asia and Australia). Supported on SRX320, SRX340, SRX345 and SRX550M
SRX-MP-LTE-AE	4G / LTE MPIM support 1-5, 7-8, 12-13, 30, 25-26, 29-30, 41 LTE bands (for Americas and EMEA). Supported on SRX320, SRX340, SRX345 and SRX550M

Accessories

Product Number	Description
SRX300-RMK0	SRX300 rack mount kit with adaptor tray
SRX300-RMK1	SRX300 rack mount kit without adaptor tray
SRX300-WALL-KIT0	SRX300 wall mount kit with brackets
SRX320-P-RMK0	SRX320-POE rack mount kit with adaptor tray
SRX320-P-RMK1	SRX300-POE rack mount kit without adaptor tray
SRX320-RMK0	SRX320 rack mount kit with adaptor tray
SRX320-RMK1	SRX320 rack mount kit without adaptor tray
SRX320-WALL-KIT0	SRX320 wall mount kit with brackets
JSU-SSD-MLC-100	Juniper Storage Unit, SSD, MLC, 100GB

About Juniper Networks

Juniper Networks challenges the status quo with products, solutions and services that transform the economics of networking. Our team co-innovates with customers and partners to deliver automated, scalable and secure networks with agility, performance and value. Additional information can be found at [Juniper Networks](#) or connect with Juniper on [Twitter](#) and [Facebook](#).

Corporate and Sales Headquarters
 Juniper Networks, Inc.
 1133 Innovation Way
 Sunnyvale, CA 94089 USA
 Phone: 888.JUNIPER (888.586.4737)
 or +1.408.745.2000
 Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
 Juniper Networks International B.V.
 Boeing Avenue 240
 1119 PZ Schiphol-Rijk
 Amsterdam, The Netherlands
 Phone: +31.0.207.125.700
 Fax: +31.0.207.125.701



Copyright 2017 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

JUNIPER
NETWORKS

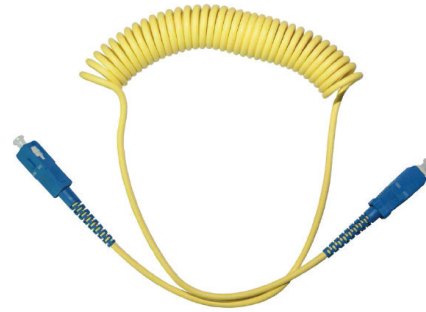
Fiber Optic Patch Cord and Pigtails

Features

- Compliance with Telcordia GR-326-Core, TIA/EIA and IEC
- Customized length
- Various connector type available
- Environmental stable

Applications

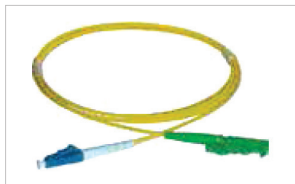
- Telecommunication network
- CATV system
- Local Area Network
- Active/Passive device
- FTTH and FTTx



Curl Cord patchcord



Pigtails



Short Boot LC



Shutter SC Connector



Drop Cable Patchcord



Uni-boot LC Connector


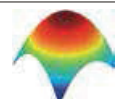




Mini-LC Connector



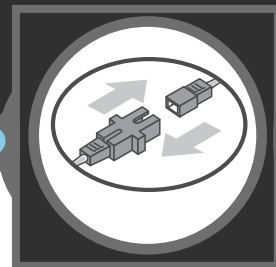


Specification

Optical Performance	Single Mode	Multi Mode		
Insertion Loss	≤0.20dB	≤0.30dB		
Return Loss	≥45dB(PC)	≥35dB		
	≥50dB(UPC)			
	≥60dB(APC)			
Repeatability	≤0.10dB			
Durability	≤0.2dB typical change,1000 matings			
Operating Temperature	- 20 ~ +75℃			
Storage Temperature	- 40 ~ +85℃			
Endface Geometry				
Parameter	2.5mm ferrule		1.25mm ferrule	
	UPC	APC	UPC	APC
Radius of Curvature	10~25mm	5~12mm	7~25mm	5~12mm
Apex Offset	0~50•m	0~50•m	0~50•m	0~50•m
Fiber Height	-100~50nm	-100~100nm	-100~50nm	-100~100nm
Angle	--	7.7-8.3degree	--	7.7-8.3degree
3D - Geometry				

Part No. Legend

000		-	00		-	00		-	00	-	0	
MODE		CONNECTOR1		CONNECTOR2		LENGTH	TYPE					
OS1	OS1	FC	FC	FC	FC	1	SIMPLEX	S				
OS2	OS2	LC	LC	LC	LC	1.5	DUPLEX	D				
OM1	OM1	SC	SC	SC	SC	2						
OM2	OM2	ST	ST	ST	ST	3						
OM3	OM3	E2000	E20	E2000	E20	5						
OM4	OM4	MTRJ	MJ	MTRJ	MJ	10						
		FC ANGLED	FCA	FC ANGLED	FCA	15						
		LC ANGLED	LCA	LC ANGLED	LCA							
		SC ANGLED	SCA	SC ANGLED	SCA							
		ST ANGLED	STA	ST ANGLED	STA							



Fiber Optic Patchcords and Pigtails

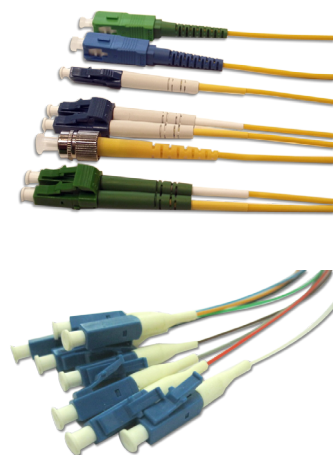
Introduction

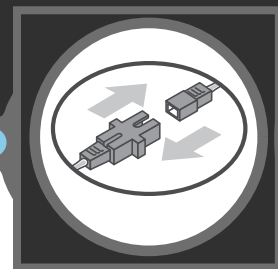
Opterna offers high performance patchcords and pigtails for use in all types of fiber optic networks. The Opterna® patchcords & pigtails are manufactured using state-of-the-art controlled manufacturing processes to operate over a wide range of wavelengths, ranging from 850nm - 1300nm for Multimode and 1310nm - 1550nm for Singlemode fiber. Opterna patchcords and pigtails are terminated with high quality connectors, which provide low insertion loss and high return loss. Each patchcord or pigtail is individually tested and supplied with test certificates. The unique serial number provides traceability of every single product.

Features

➤ Patchcords and Pigtails

- Available in singlemode and multimode fiber types
- Available with all fiber optic connector types
- High quality ferrules and housings
- Low insertion loss and high return loss
- Individual test results and unique trace number provided with every product
- Mating Durability: 1000 cycles; <0.2 dB change
- Temperature range: -40 °C to +70°C
- RoHS compliant
- IEC, EIA/TIA and GR-326-CORE compliant





Fiber Optic Patchcords and Pigtails

Applications:

- Datacenter and Datacom
- FTTX deployments
- Pre-terminated assembly interconnection
- CATV, WAN, LAN and Telecom networks
- Testing and measurement equipment

Size & Dimensions:

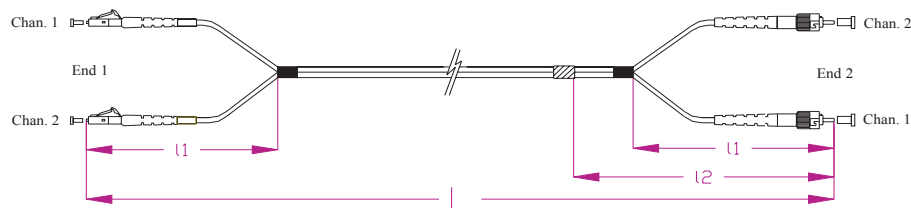


Fig.1: Duplex patchcord schematic

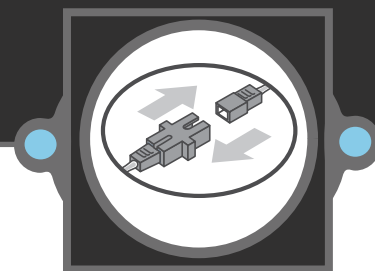


Fig.2: Simplex patchcord schematic



Fig.3: Pigtail schematic

Length of assembly (L)	L -0/+100mm (for L<0.5m)
	L -0/+150mm (for 0.5m>L<5m)
	L -0/+200mm (for L>5m)
Split length (l ₁) - only for duplex	150 ± 25mm
Traceability label distance (l ₂)	200 ± 25mm (from one end)



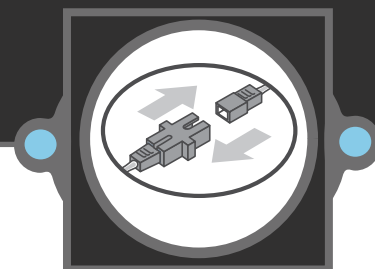
Fiber Optic Patchcords and Pigtails

General Specification:

Parameter	Specification
Fiber Types	Multimode: OM1, OM2, OM3, OM4
	Singlemode: G652D, G657A1, G657A2, G657B2, G657B3, G655
Cable type	Simplex: 2.8, 2.0, 1.8, 1.6, 1.2, 0.9, 0.6, 0.250mm
	Duplex: 2.8, 2.0, 1.8mm
	Flat duplex: 2.8mm
Cable Colours	Blue, Yellow, White, Orange, Aqua, Heather Violet
Connector Types	SC, LC, MU, FC, ST, MTRJ, ESCON, E-2000, SMA, FDDI
Endface Finish	PC, UPC, APC

Optical performance specification:

Parameter	Connector Type	Max	Typical
Insertion loss (dB)	Multimode SC, LC, MU, FC, ST, E-2000, ESCON, FDDI	0.30	0.20
	Multimode MTRJ & SMA	0.75	0.50
	Singlemode SC, LC, MU, FC, ST, ESCON, FDDI	0.30	0.20
	E2000	0.25	0.12
	MTRJ	0.50	0.30
Return Loss (dB)	All types Singlemode UPC endface finish type	50	55
	All types Singlemode APC endface finish type	60	65



Fiber Optic Patchcords and Pigtails

Ordering Info:

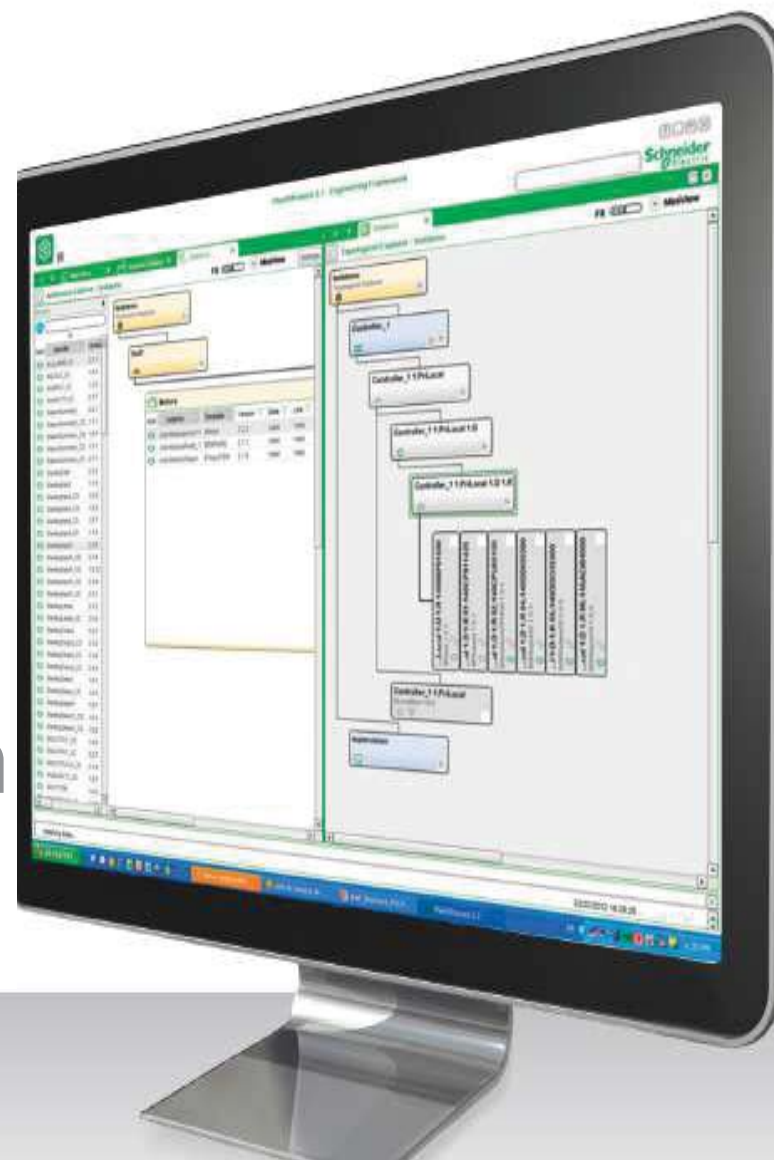
CA																																									
Connector Type End 1		Connector Finish End 1		Cable Diameter		Fiber Type		Cable Type		Cable Material		Connector Type End 2		Connector Finish End 2		Cable Length		Cable Colour																							
ST	ST connector	P	PC	16	1.6mm	OM1	62.5/125 MM	SX	Simplex	L	LSZH	ST	ST connector	P	PC	005	0.5 meter	BL	Blue																						
SC	SC connector	U	UPC	18	1.8mm	OM2	50/125 MM	DX	Duplex	V	PVC	SC	SC connector	U	UPC	015	1.5 meter	YL	Yellow																						
SD	SC duplex	A	APC	20	2.0mm	OM3	50/125 MM Laser Optimized	FD	Flat Duplex	R	RISER	SD	SC duplex	A	APC	150	15 meter	WH	White																						
FC	FC connector			28	2.8mm	OM4	50/125 MM Laser Optimized	TB	Tight Buffered	P	PLENUM	FC	FC connector	Blank for pigtail				OR	Orange																						
LC	LC connector			02	250um	OS2	9/125 SM G.652D	ES	Easy strip			LC	LC connector					AQ	Aqua																						
LD	LC duplex			06	600um	7A1	G-657A1 SM Bend insensitive	LT	Loose tube			LD	LC duplex					HV	Heather Violet																						
MU	MU connector			09	900um	7A2	G-657A2 SM Bend insensitive					MU	MU connector																												
MD	MU duplex			12	1.2mm	7B2	G-657B2 SM Bend insensitive					MD	MU duplex																												
E2	E-2000 connector					7B3	G-657B3 SM Bend insensitive					E2	E-2000 connector																												
MT	MTRJ connector					655	9/125 SM G-655					MT	MTRJ connector																												
FD	FDDI connector											FD	FDDI connector																												
ES	ESCON connector											ES	ESCON connector																												
SM	SMA connector											SM	SMA connector																												

ATTACHMENT 1 – CATALOGUE AND DATASHEET

SOFTWARE

Process Expert System

Commercial offer for PES V4.3





Confidential Property of Schneider Electric | Page 2

1 PES Architecture Overview

2 Software Offer Description / Licenses

3 Support Services

4 Updating PES to V4.3

5 Licensing Embedded Virtual Machines

6 PlantStruxure PES Libraries Overview

Life Is On

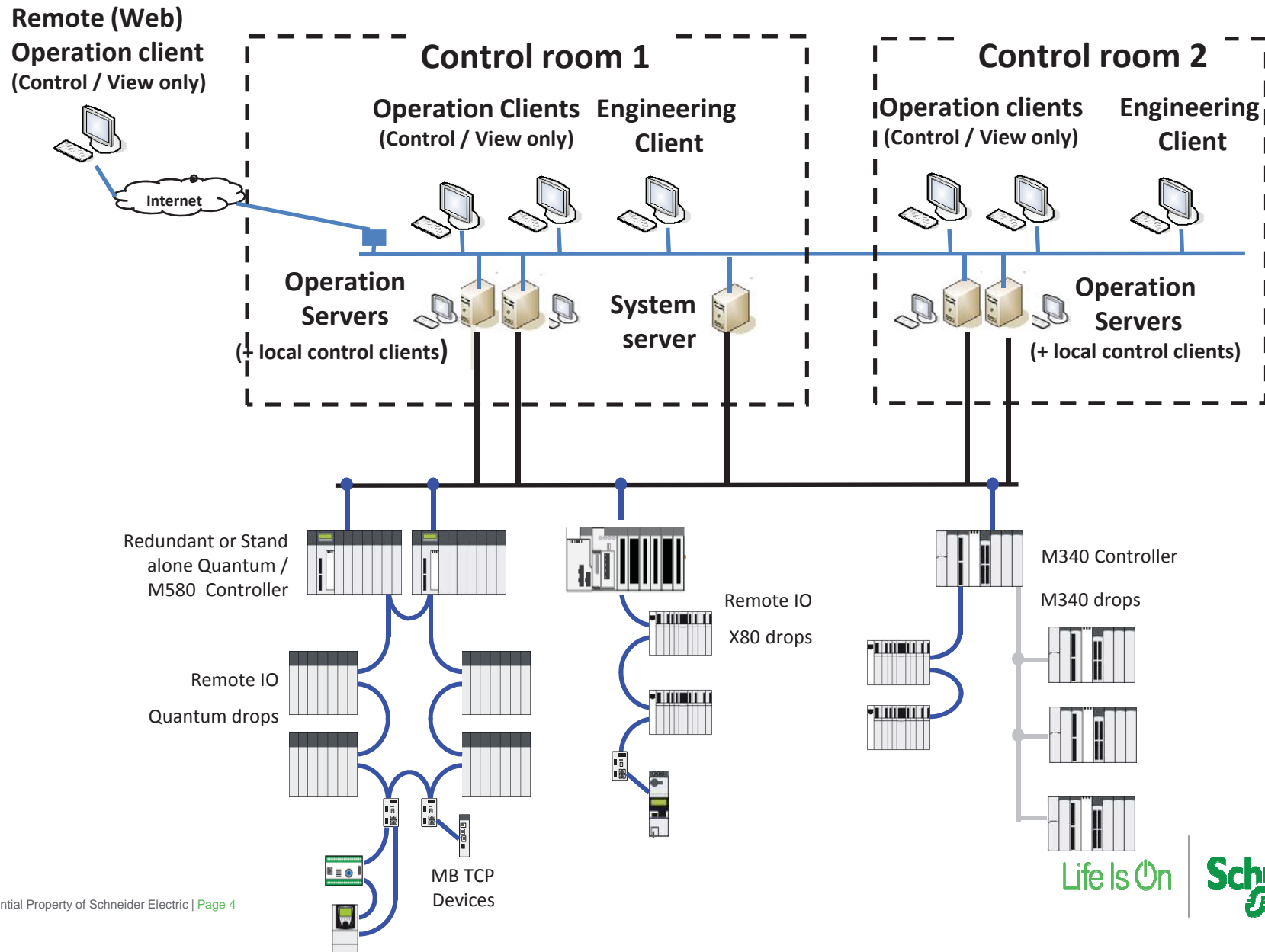
Schneider
Electric



The image shows a person from behind, sitting at a desk in a control room. They are looking at several computer monitors. The leftmost monitor displays a table with multiple columns of data, likely a process log or inventory list. The central monitor shows a complex industrial process diagram with various tanks, pipes, and valves, overlaid with numerical data points. The rightmost monitor shows another data table. On the desk in front of the person is a black office chair, a multi-line office phone, and a white hard hat. The background shows a modern office environment with glass partitions.

PES Architecture Overview

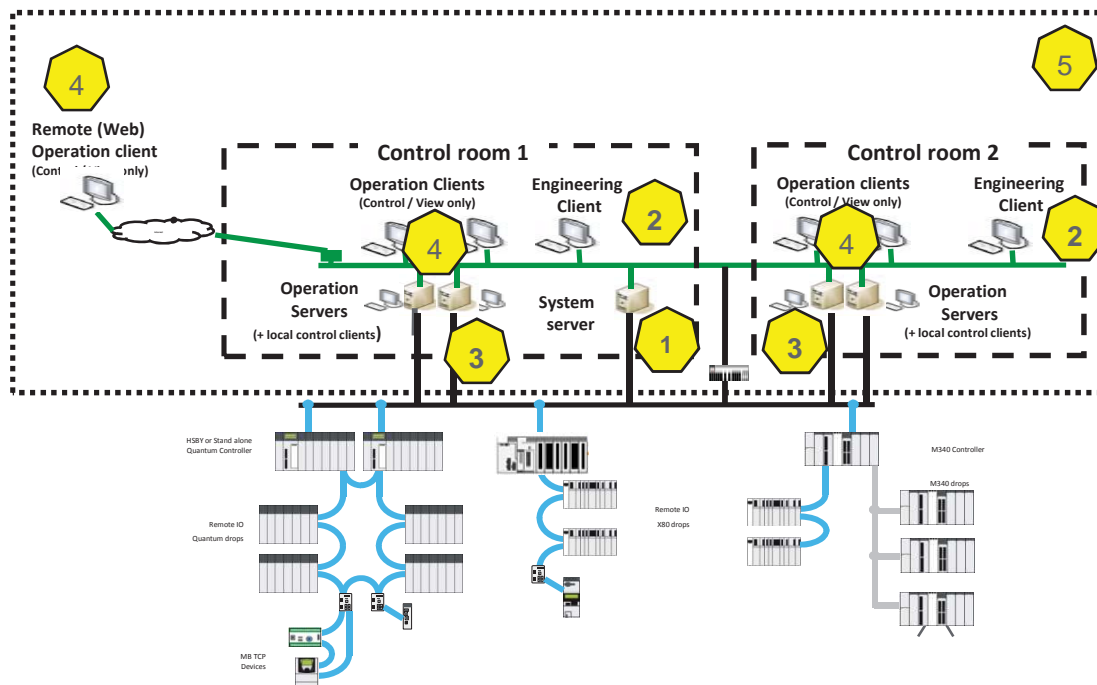
Control system infrastructure



PES software licenses at a glance

Each software component of the PES infrastructure requires a license to run

- Five software components are required for any PES configuration



PES System server (mandatory)

- Core of the configuration
- Store applications and Eng tools
- Enabling Runtime Services

Engineering client(s)

- Mandatory to engineer / modify the deployed application
- One is bundled with the System server

Operation server(s) (1 is mandatory)

- Functions of IO data gathering, alarming, historize and reporting

Operation client(s) (1 is mandatory)

- User interface for operators
- Entry point for runtime services
- Control client / view only client
- Local /remote & Web client

Application license (mandatory)

- One license per configuration
- 5 levels, depending on the number of object instances



Software Offer Description / Licenses



System Server

The System Server is the core component of PES infrastructure

- Repository of the Control System Application
- Server + one Client minimum are required to engineer the control system application
- It embeds the “Software Participants” within a Virtual Machine
 - Control builder (Unity Pro & Advantys Config Software)
 - Graphic builder (Vijeo Citect)
- Navigation: Access from one object selected in the Supervision to all the related information linked to this object (other object instances and the logic in a controller that manages this object)
- The license enables the server and one Engineering client
 - The client can be local on the same machine or remote

Part number

System Server + Client Eng

EUSBEUCZZSXZZ

Engineering clients

The Engineering Client is the user interface to engineering a control system application

- Can be installed on the same workstation as the System Server
 - One Eng client is bundled with the System Server license
- Can be installed on another workstation (alone or combined with the Operation Client)
- Multiple Engineering Clients can access concurrently to the same System Server, enabling concurrent design
 - On different control system applications
 - Shared design of a control system application

Three part numbers, depending on the number of rights for engineering clients

Reminder

Single: 1 license
Group: 3 licenses
Team: 10 licenses

Part Number	
“Single” license	EUSCLTCZZSPEZZ
“Group” license	EUSCLTCZZGPEZZ
“Team” license	EUSCLTCZZTPEZZ

Application license

Application license

- **Mandatory** with the appropriate size to open a Control System Application
- One Application license for one PlantStruxure PES infrastructure
- Pricing based on the Application size: Size is based on the maximum of object instances that can be created in all the control system applications that are currently stored in the PlantStruxure PES

5 part numbers for the sizes / 4 part numbers for upgrades of the size

Size	Nb object instances	Part Number		Upgrade PN
X Large	Unlimited	EUSAPPCZXSPEZZ	↑	EUSAPPGZKSPEZZ
Large	7500	EUSAPPCZLSPEZZ	↑	EUSAPPGZHSPEZZ
Medium	3000	EUSAPPCZMSPEZZ	↑	EUSAPPGZESPEZZ
Small	1250	EUSAPPCZSSPEZZ	↑	EUSAPPGZASPEZZ
X Small	500	EUSAPPCZTSPEZZ		

Operation server and clients

Operation Server

- One Operation Server is **Mandatory**
- In case of redundancy, multiply by two (no additional part)
- The Server embeds one local Client (on the Server machine)

Operation Clients local or remote (Web Clients)

- Minimum one client in the configuration
 - Can be the local Client on the server
- Operation **Control Client**
 - Recommended to control the system
- Operation **View only client**
 - Don't allow any modification
- Web Clients support only supervision services (no RTNS)

Part numbers

	Part Number
Operation Server	EUS O PECZZSPEZZ
Operation Control Client	EUS L CCCZZSPEZZ
Operation View Only Client	EUS V CCCZZSPEZZ

Configurations with redundant Operation servers

Redundant Operation servers

- Multiply by two the Qty (no additional part)
- Licensing: Primary and Secondary Server must embed one floating license manager each with its license and the Client licenses to ensure the availability of the supervision at any time

Operation clients local or remote (Web clients)

- For each Control or View only client, order a couple of licenses (standalone + redundant) to get a license for the client at any time in case of failure of one Operation Server

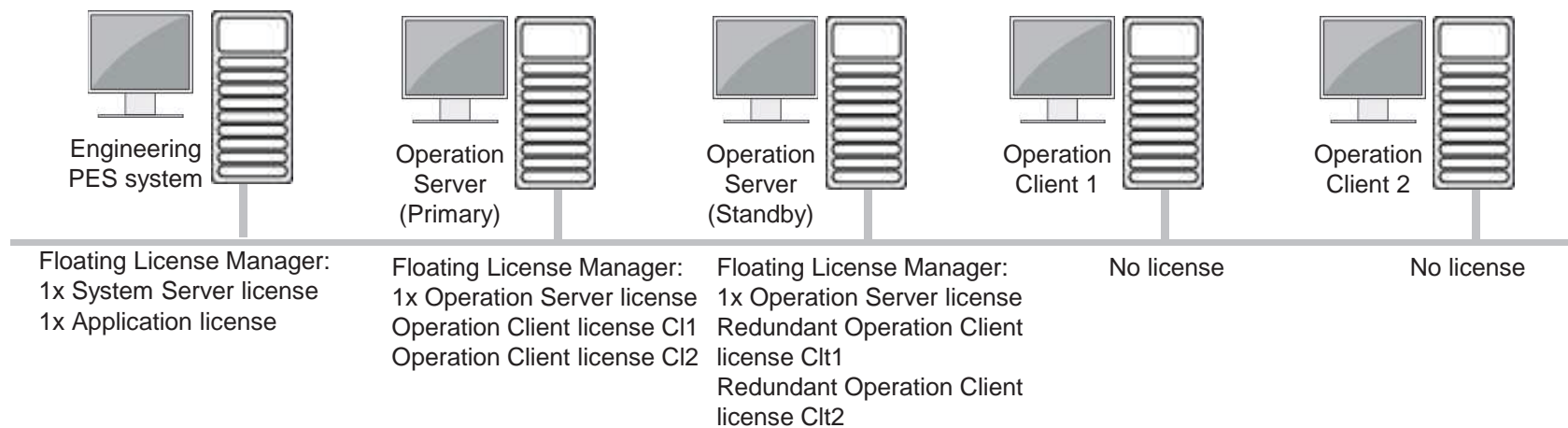
Part numbers

	Part Number (Standalone license)	Part Number (Redundant license)
Operation Control Client	EUSLCCZZSPEZZ	EUSLRCZZSPEZZ
Operation View Only Client	EUSVCCZZSPEZZ	EUSVRCZZSPEZZ

- Redundancy of the System Server is not available with this release

Example of licensing of redundant Operation Servers

- One workstation embedding the System Server + one Engineering Client
- Two Operation servers (redundant)
- Two operation clients



How to license a software configuration?

Non redundant Operation Servers

EUSBEUCZZSPEZZ

+

EUSCLTCZZ(x)PEZZ

+

1 x

EUSAPPCZ(x)SPEZZ

+

m x

EUSOPECZZSPEZZ

+

n x

EUSLCCCZZSPEZZ

+

p x

EUSVCCCZZSPEZZ

+

q x Window 7 licenses

- **The System Server is mandatory**

- One only possible with V4.0 (no redundancy)

- **Check the number of Engineering clients required**

- One is provided with the System Server license
- Single (x1), Group (x3), Team (x10)

- **Check the number of instances required to define the Application license**

- Make the choice among five sizes

- **Check the topology and the size of the application to define the number of operation servers**

- Minimum one server

- **Check the number of operation stations required**

- # Control clients / # View only clients
- Local client on the Operation server can be used as a Control Client

m: number of Operation servers

n: number of Operation Control Clients

p: number of Operation View Clients

- **Check how many Microsoft Windows 7 licenses are required for the virtual machine**

How to license a software configuration?

Redundant Operation Servers

EUSBEUCZZSPEZZ
+
EUSCLTCZZ(x)PEZZ
+
1 x
EUSAPPCZ(x)SPEZZ
+
2 x m x
EUSOPECZZSPEZZ
+ **n x**
(EUSLCCCZZSPEZZ
+
EUSLRCCZZSPEZZ)
+ **p x**
(EUSVCCCZZSPEZZ
+
EUSVRCCZZSPEZZ)
+
q x Window 7 licenses

- **The System Server is mandatory**
 - One only possible with V4.0 (no redundancy)
- **Check the number of Engineering clients required**
 - One is provided with the System Server license
 - Single (x1), Group (x3), Team (x10)
- **Check the number of instances required to define the Application license**
 - Make the choice among five sizes
- **Check the topology and the size of the application to define the number of operation servers**
 - Double the quantity of servers for redundancy
- **Check the number of operation stations required**
 - # control clients / # View only clients (LCC/VCC)
 - Each control client requires a redundant license (LRC/VRC)
 - Local client on the operation server can be used as a Control Client
- **Check how many Microsoft Windows 7 licenses are required for the virtual machine**

m: number of Operation servers

n: number of Operation Control Clients

p: number of Operation View Clients

All-in-one: PES Mini

PES configuration dedicated to a very small project

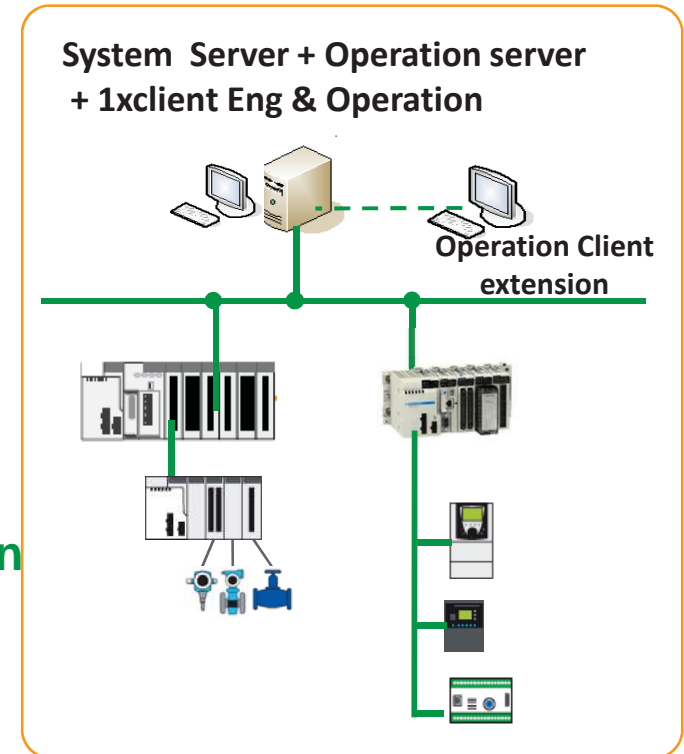
- Systems with 3 controllers maxi (typ)
- Limited to 200 object instances
- No redundancy
- Extensible only with operation clients
- Upgrade possible to 500 object instances maxi

All-in-One on a single computer

- Engineering the control system
- Operation and Maintenance

Same services as the bigger PES configuration

- Engineering and runtime services
- Embedded GPL libraries



Part numbers

PES Mini (200 obj instances)

Upgrade PES Mini (to 500 obj instances)

Part Number

EUSMINCZTSPEZZ

EUSMINGZASPEZZ

Configurations for engineering

Offers for Application Service Centers and System Integrators

- Pack of 1, 3, 10 licenses (seats) dedicated for projects
- Unlimited number of object instances for control systems
- Include build time and runtime services (8 continuous hours)

Offer of Alliance Partners (option to the Alliance Partner Program)

- System Integrators who joined the Alliance Partners program
- Same license profile as other offers, but limited to 12 months

Part Numbers

Reminder

Single: 1 license
Group: 3 licenses
Team: 10 licenses

One activation ID for
Group & Team licenses
(multiple activations with
the same ID)

For Application Execution Centers

Part Number

Single license	EUSBASCZZSPEZZ
Group license	EUSBASCZZGPEZZ
Team license	EUSBASCZZTPEZZ

For System Integrators

Part Number

Single license	EUSSISCZZSPEZZ
Group license	EUSSISCZZGPEZZ
Team license	EUSSISCZZTPEZZ

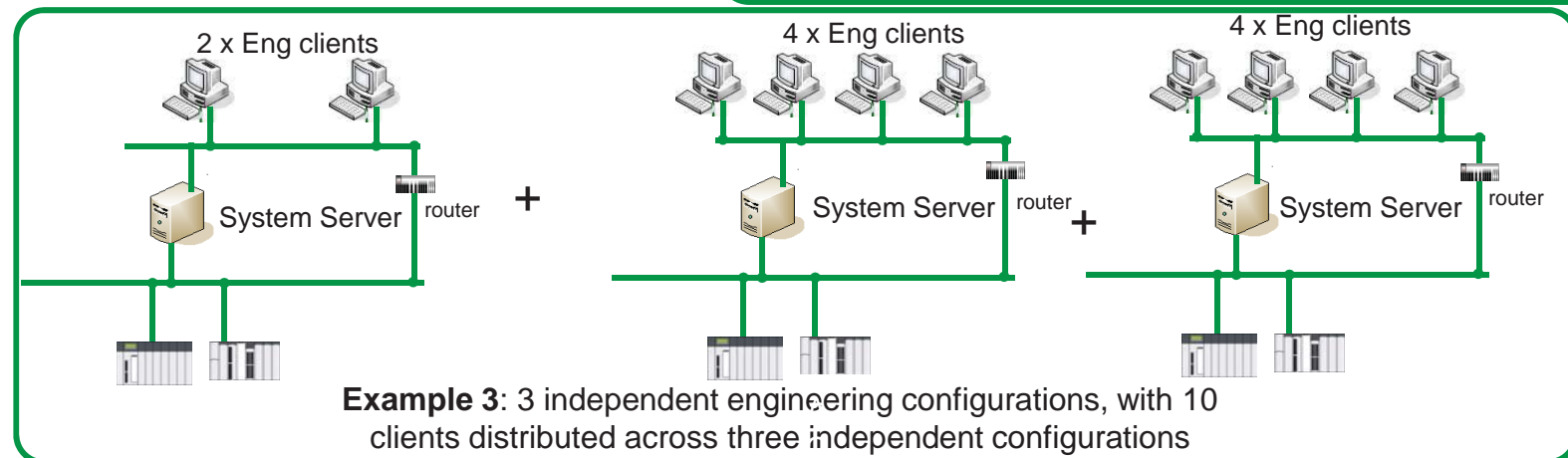
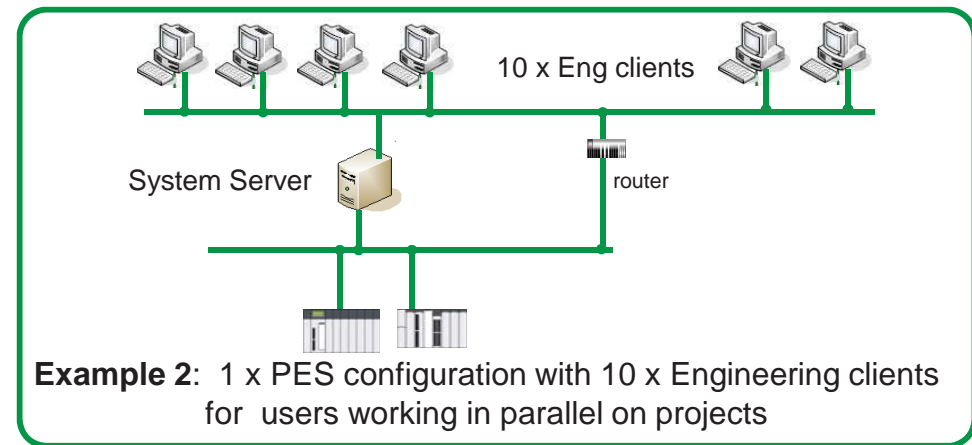
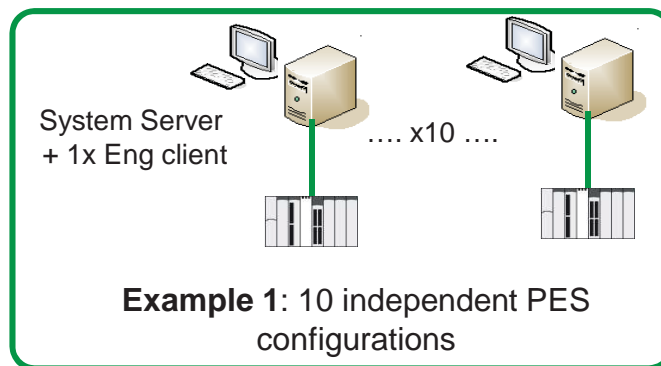
For Alliance Partners

Part Number

Group license	EUSBALCZZGXEZZ
---------------	----------------

Engineering configurations; Examples

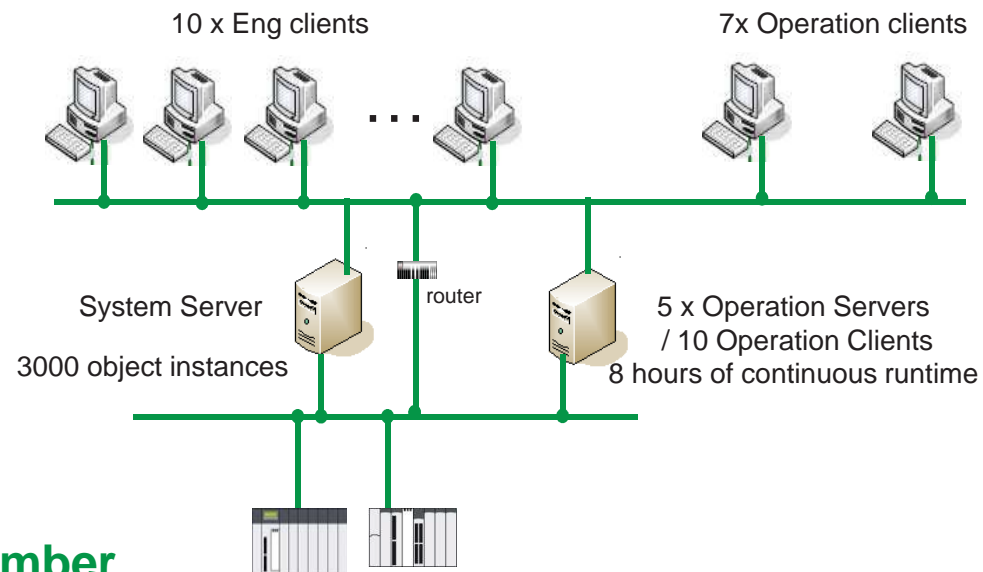
- A multiple seats license enables several possibilities of configuration. The rule is not exceeding the number of seats for System Servers and the number of seats for engineering client licenses allowed by the part number.
- A Team license embeds 10 license rights for the System Server and 10 license rights for the engineering clients
- Possibility to add additional Engineering clients (to be ordered separately)



PES for Education

Offers dedicated to educational entities

- For trainings and design of applications dedicated to education purpose
- Based on one System Server and 10 Eng clients maximum
- Include 3000 object instances maximum
- Include build time and runtime services (8 continuous hours)



Part Number

PES for Education

Part Number

EUSBASEZMSPEZZ

PES for demonstration

Software license for Sales

- Only available for Schneider personnel for demonstration purpose
- Cannot be used by an external entity (End User or System Integrator)
- Include build time and runtime services (8 continuous hours)
- Includes 500 object instances maximum

Part Number

Part Number	
PES for Sales	EUS SL VZZSPEZZ

Ordering & registering licenses

Ordering

- Mandatory through eMRO
- A training to « One Licensing » is mandatory prior the first order

Registration

- Through the License Manager, which is installed with PlantStruxure PES
- Three modes of registration:
 - Through Web (need an Internet connection); easiest way & immediate
 - Software Licensing portal (through another PC with access to the Internet)
 - Through eMail; require more than one day to activate a license

Policies applicable to the licenses

- “Rehost”: Return back the license on the Software Licensing Portal
- “Repair”: Following a crash of the workstation, to recover the license on the same machine
- “Reinstall”: Following a crash of the workstation, recover the license on another machine (need assistance of the Software Registration Center)

Floating license	Single	Group	Team
Nb of Rehost / year	7	9	20
Nb of Repairs / year	3	4	5
Nb of Reinstalls / year	3	4	5

Licenses management

The owner of a PES license can rely on the Software Licensing Portal to administrate his licenses

Support - Software Licensing

You are here: Home > Support > Software Licensing

Software Licensing Web Portal

To know more

- PlantStruxure PES
- Power Monitoring Expert
- Vjeo Citect
- Vjeo Historian

Manage my licenses

Search by Activation ID or Entitlement ID

A-PULK-CFDG-YEB8 **Search**

1 - 1 of 1 View: 10 per page

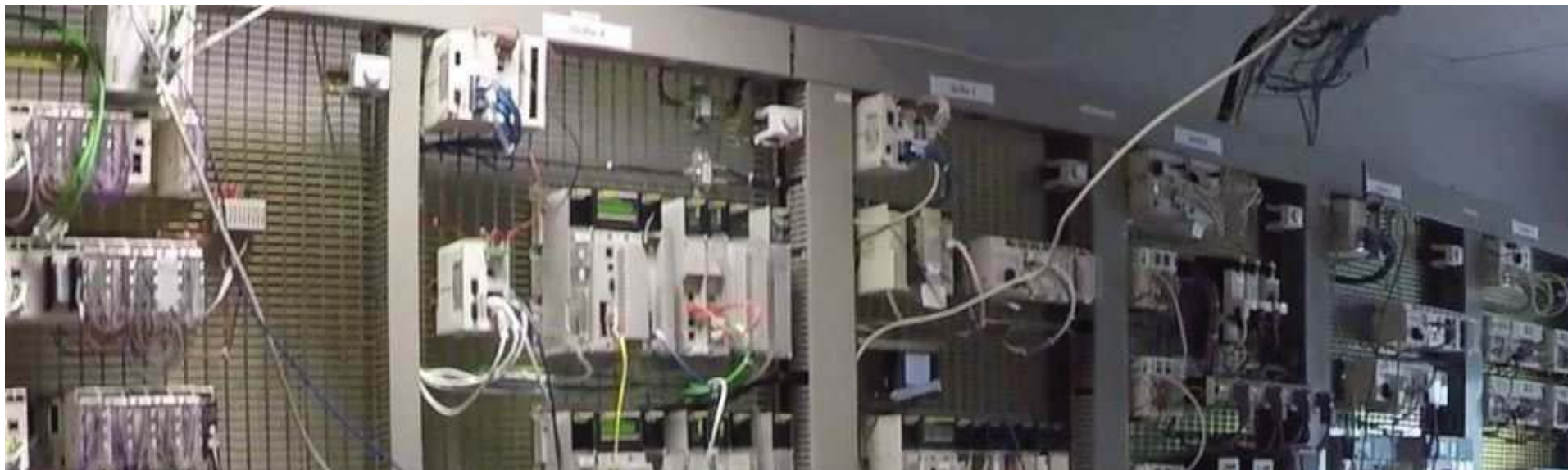
+	Activation ID	Product	Part Number	Usage Rights	License Status
+	A-PULK-CFDG-YEB8	SWPE_SALES Version 3.1	EUSSLCZZSRE31	1/1	

StruxureWare Process Expert Engineering SALES: includes
License Type: Floating without borrowing

Duration: 3 months

Please activate your license.

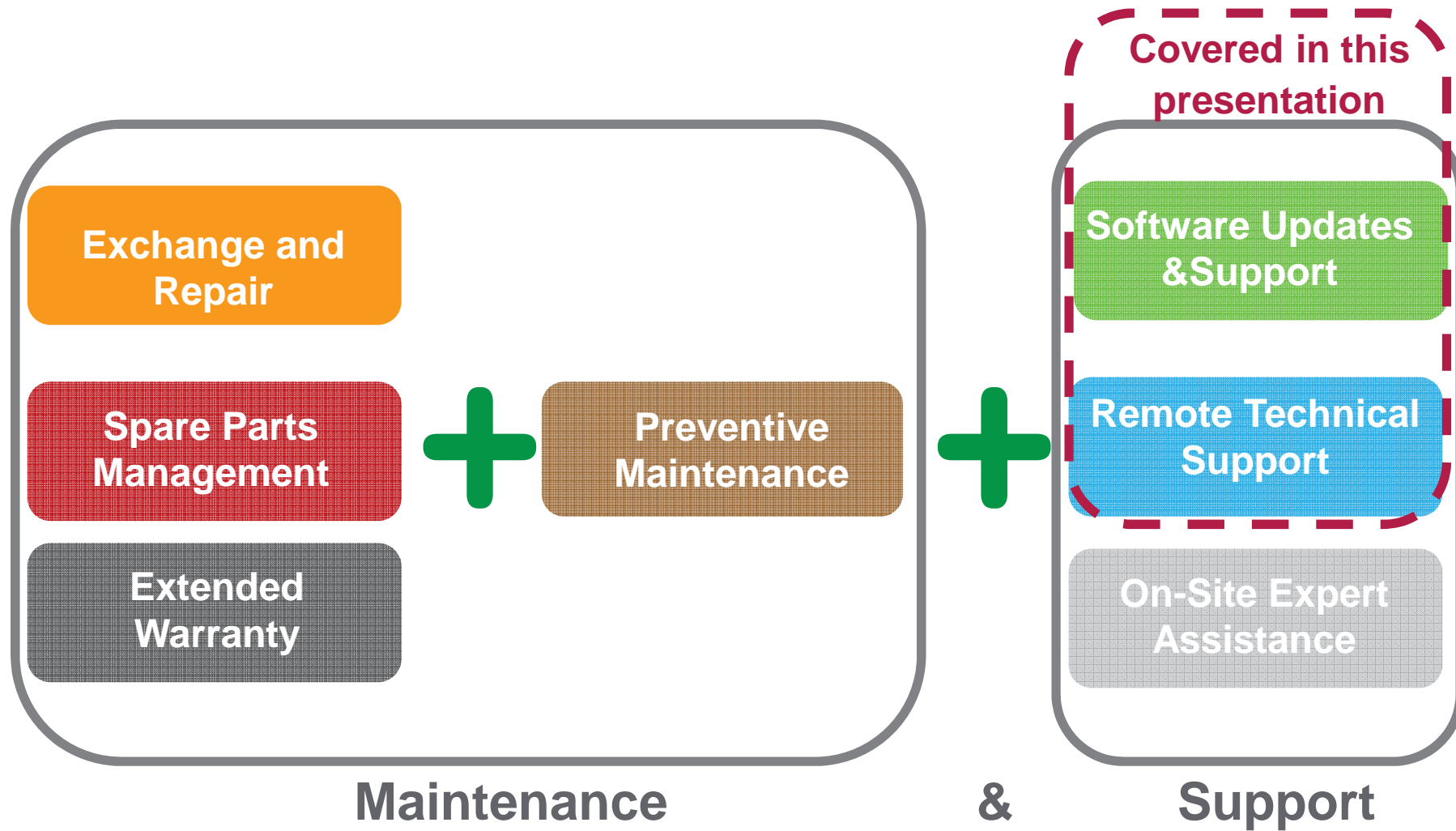
On www.schneider-electric.com ; Support / Software Licensing



Support Services



A range of services tailored to accommodate various requirements



Software updates and remote technical support

Selling service support with licenses brings benefits to our customers

- Major cost savings
- Improved production performance
- Expert and professional support - receive fast and accurate answers
- Access to version upgrades (1+ release per year)
- Protect their automation investment

Three levels of support

- The licenses are not bundled with any support or update
- It is mandatory to sell « Silver » support minimum with the licenses

Service Name	Gold Plus	Gold	Silver
Services			
Telephone support	24x7	8x5	8x5
Software upgrades	Yes	Yes	No
Support portal	Yes	Yes	Yes

Support service

This is more than support phone calls



Escalation process to manage Customer requests



Service offer quotation

Calculation based on the licenses that are running on a site

- A site contains all the PES server, Engineering clients, Operation servers and Operation clients
- The definition of a site is regardless how the software pieces are distributed in one or several locations, for example in control rooms.
- Each software licenses has a value in term of Support Units
- Each level of service has an Unit Price
- Calculation of the Support Fee:

Support fee (for 12 months) = Unit Price x Quantity

- Unit Price = Unit price of the Support level purchased
- Quantity = Total Support Units for the software licenses

Ordering must be done through SOC (Sales Ordering Configuration)

- From the list of licenses entered, SOC calculates the Support fee to place to place the order

Part Numbers

	Part Number
Silver Service (Unit Price)	EUS001
Gold Service (Unit Price)	EUS011
Gold Plus Service (Unit Price)	EUS012

Updating PES to V4.3

Updating to PES V4.3

Two ways for updating the PES licenses

- The customer has a service contract that includes updates (Gold / Gold Plus)
 - He can update the licenses through the PES Support Web portal
 - License generator enables to get the update
- The customer doesn't have any service contract, or has a Silver contract
 - He can buy an update for each individual license
 - The update doesn't include any support service

A Service contract is less expensive than buying updates

- Price of an update = Price of Gold service for the license

Exceptions: “Sales”, “Alliance”, “Schneider Execution centers” licenses

- Free update for “Sales” license
- 12 months free update for “Alliance” & “Schneider Execution centers” licenses
- Renewal of the Alliance partnership contract is required for Alliance
- Renewal of Schneider Application center license through Gold service

Update a former license to V4.3

An easy way to know the updates PN:

- Replace the 7th digit of the PN ("C" with "D")

License V3.1, V4.0, V4.1, V4.2	Update V4.3 to be ordered
EUSMINCZTSPEZZ	EUSMINDZTSPEZZ
EUSMINCZTSPEZZ + EUSMINGZASPEZZ	EUSMINDZSSPEZZ
EUSBEUCZZSPEZZ	EUSBEUDZZSPEZZ
EUSCLTCZZSPEZZ	EUSCLTDZZSPEZZ
EUSCLTCZZGPEZZ	EUSCLTDZZGPEZZ
EUSCLTCZZTPEZZ	EUSCLTDZZTPEZZ
EUSAPPCZTSPEZZ	EUSAPPDZTSPEZZ
EUSAPPCZSSPEZZ	EUSAPPDZSSPEZZ
EUSAPPCZMSPEZZ	EUSAPPDZMSPEZZ
EUSAPPCZLSPEZZ	EUSAPPDZLSPEZZ
EUSAPPCZXSPEZZ	EUSAPPDZXSPEZZ
EUSOPECZZSPEZZ	EUSOPEDZZSPEZZ
EUSLCCCZZSPEZZ	EUSLCCDZZSPEZZ
EUSLRCCZZSPEZZ	EUSLRCDZZSPEZZ
EUSVCCCZZSPEZZ	EUSVCCDZZSPEZZ
EUSVRCCZZSPEZZ	EUSVRCDZZSPEZZ
EUSSISCZZSPEZZ	EUSSISDZZSPEZZ
EUSSISCZZGPEZZ	EUSSISDZZGPEZZ
EUSSISCZZTPEZZ	EUSSISDZZTPEZZ

Licensing Embedded Virtual Machines

Why licensing Virtual Machines?

PES architecture embeds Virtual Machines (VMs) depending on the services provided by the software component

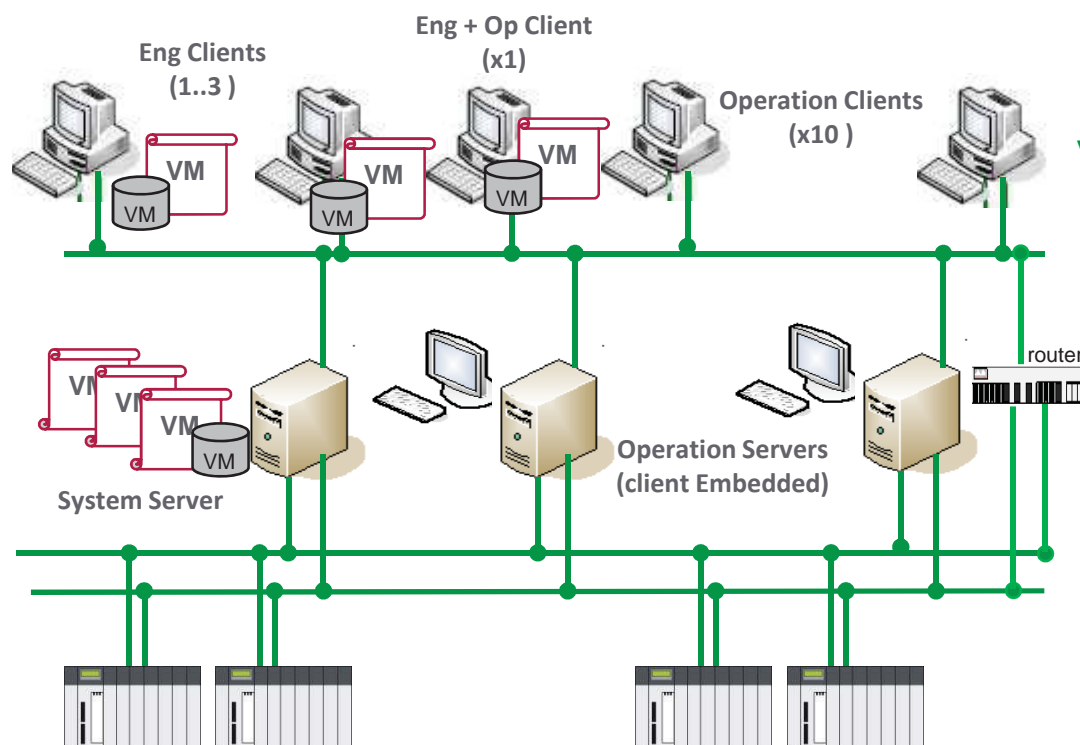
- Engineering: running Control builder (Unity Pro), Supervision graphic builder (Vijeo Citect), Advantys Configuration software as software participants in a Virtual Machine
- Operation: get advanced diagnostics and access to the root cause of failure through the Runtime Navigation Services (RTNS)

Number and location of the VMs need to follow the recommendations:

- A VM must be installed on each engineering client
- Never installed on an Operation client, except if the machine embeds also an engineering client
- Never installed on an Operation server
- One or many on the System Server, to benefit of the Runtime Navigation Services. As many as the number of Operation Clients that accesses simultaneously to the controller program for diagnostics.
 - Typically: 1 VM instance licensed for 4 operation clients

Example of PES configuration

Location of the Virtual Machines



Virtual Machine(s): nb & location

- 1 x VM on each Eng client
- 1x VM on the Eng + Oper client
- 1x to 10x VM licenses on the system server; Typ: 3 licenses to get concurrent access to controller programs from 3 operation clients simultaneously

Licensing Virtual Machines; possibilities offered by Microsoft

Virtual Machines running on Windows Pro are licensed through a software contract, which must be contracted through a Microsoft distributor; two possibilities:

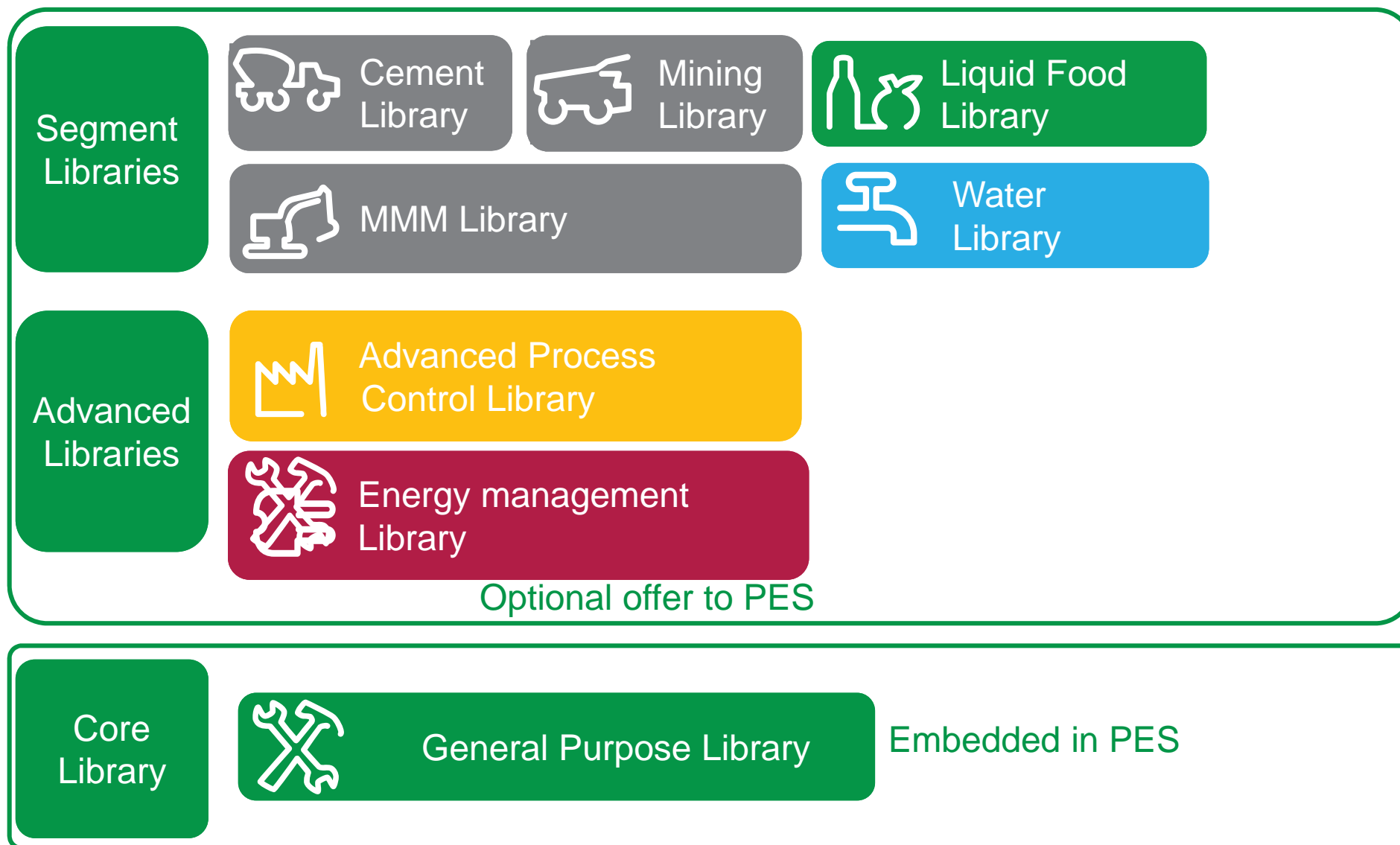
- Software Assurance (SA) is subscribed for a duration of 3 years mini. Within this contract, the customer orders the number of licenses for each software products that will be used on site. The SA includes the maintenance.
 - To run PES, Windows must be included in the SA contract. The user has to order the number of licenses that are required for his configuration
- The customer buys a contract “Select” or MPSA” and includes the number of “CAL VDA” for Windows Pro required for PES
 - CAL VDA is included inside the Software Assurance
- In each case, the user pays a fee per month. The right to run the software remains valid as long as the contract is active (not infinite duration license)



PES Libraries Overview

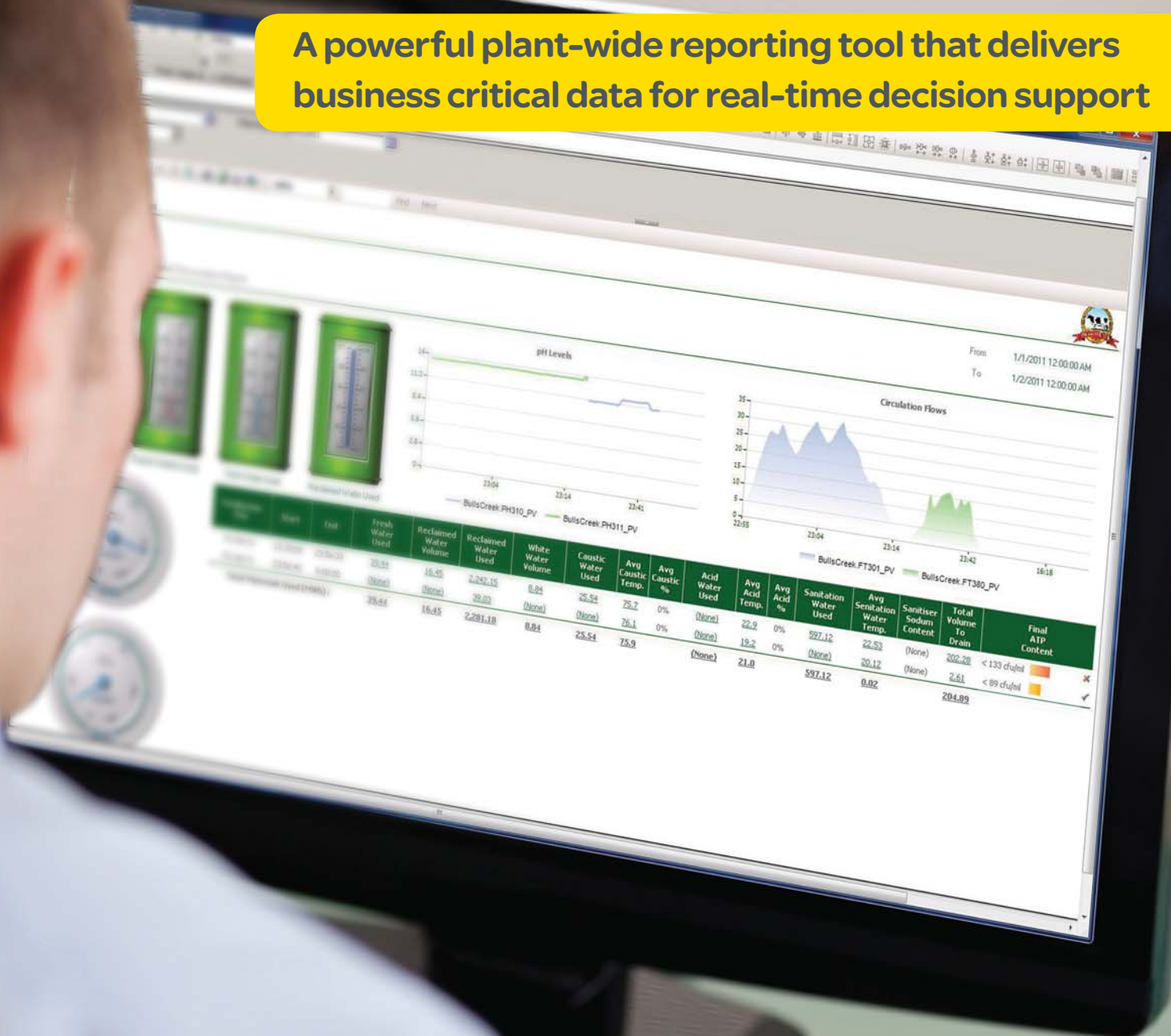


A set of libraries, ready to configure



CitectHistorian Technical Overview

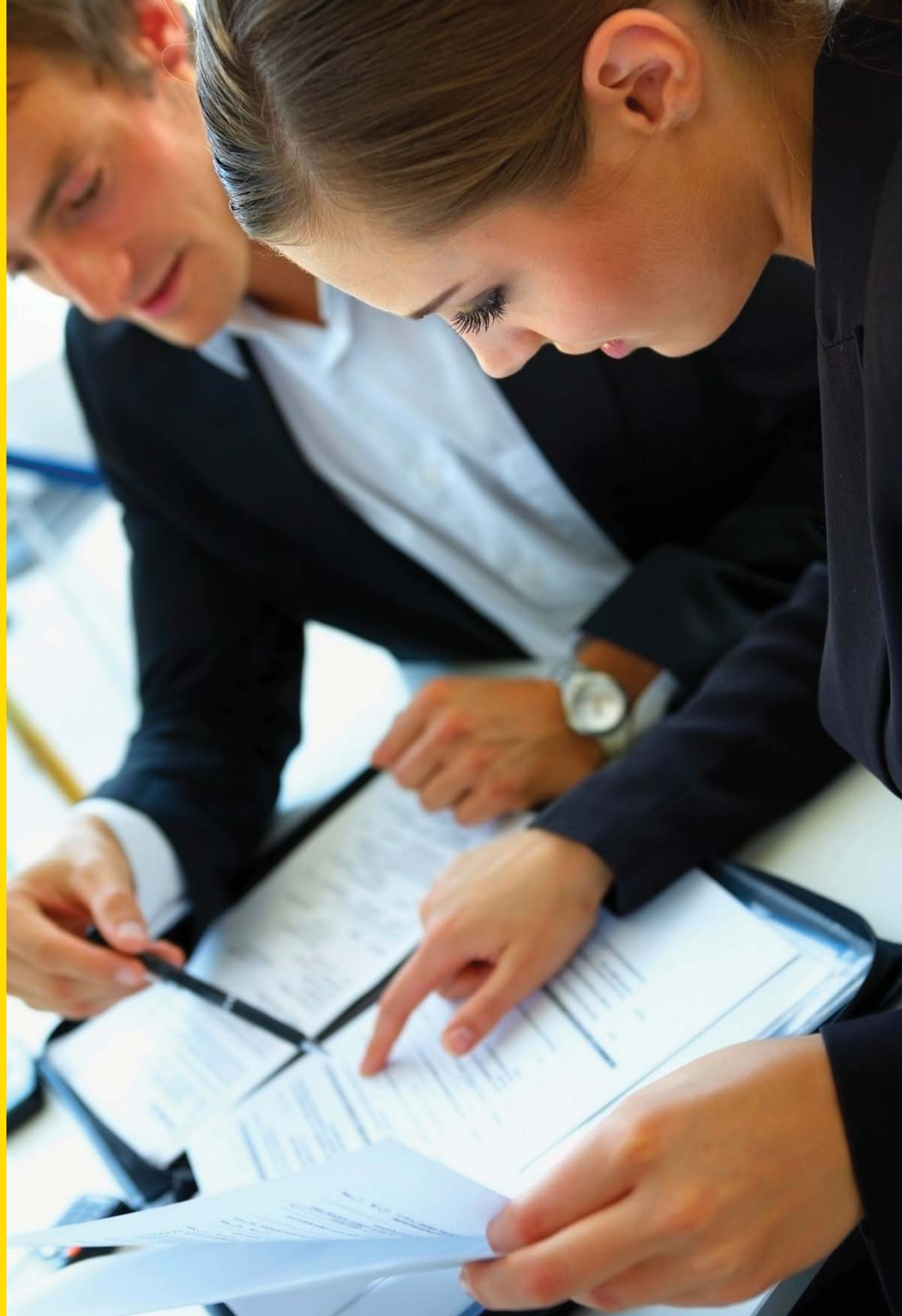
A powerful plant-wide reporting tool that delivers business critical data for real-time decision support



Schneider
Electric



Your data - how you like it	4
What is CitectHistorian	5
High performance	6
CitectHistorian Server	7
Universal connectivity	8
Historian architecture	10
Data analysis	12
Process Analyst	15
Improve operations with Process Analyst	16
Data exchange and integrity check	18
Flexible configuration	20
Data access via Web and Excel Clients	22
SCADA & MES Software Global Support	24
Customer Service Resolution	26
Educational Services	27



At a glance

- > Integrates tightly with your CitectSCADA system. The data collected in CitectHistorian includes any tags within the control system, and alarms and events from SCADA systems.
- > Can be automatically configured and synchronized with your CitectSCADA system for reduced setup costs and maintenance
- > Utilizes Microsoft® Office Excel® for simplified, ad hoc analysis and basic reporting
- > Incorporates Microsoft SQL Server® 2008 R2 as the embedded data store
- > Powerful, easy-to-use reporting tools
- > Intuitive visualization tool, Process Analyst, to easily view and analyze plant processes on a single, integrated display
- > Out-of-the-box sample reports, such as alarm management reports based on EEMUA 191 guidelines, and energy reports
- > Open technology bridges plant to business divide
- > Easy to install, configure, use and maintain
- > Improves plant efficiency with better access to information for effective decision-making
- > Reduce costs through the use of open, standard technologies and desktop applications
- > Integrates with existing ERP/MES systems

Your data - how you like it

In the demanding world of continuous process control, accessing accurate and timely plant data is crucial. As your systems grow, so does the volume of process data and the demand to translate it into relevant and actionable information for operations and management staff. Yet too often, organizations struggle with connecting and retrieving the relevant information from their plant and IT systems. When they do succeed, often managers cannot make effective use of the core manufacturing data, essential for controlling operating costs, because the data is too complex.

CitectHistorian helps your plant and IT personnel to optimize operational efficiency by providing a powerful, plant-wide reporting tool that collects, and delivers meaningful reporting data from multiple, disparate systems. By using the information provided by CitectHistorian, you will be able to make more effective decisions toward optimizing operational performance.

Comprising of historian and client functionalities, CitectHistorian enables you to accurately store data for long-term reporting while also giving you the option of visualizing and accessing the information through the CitectHistorian client, Microsoft Excel or Reporting Services.

CitectHistorian improves production reporting and ad-hoc analysis by connecting, aggregating and presenting real-time information from multiple disparate systems throughout the plant, allowing corporate, IT, plant and production managers to make more informed and timely decisions.

Based on open, standard technologies, CitectHistorian integrates your plant and business information systems to facilitate improved decision-making, leading to increased production and profitability.

An inclusive, secure and open platform, CitectHistorian allows controlled access to both plant floor and business database information by any division within your organization, and in a context that is tailored to each individual.

Using familiar, easy-to-use tools and processes, production, quality assurance, maintenance and sales can access the latest information using a wide selection of viewing clients.

Link every aspect of your business, from the plant floor right through to remote web clients, without disrupting the daily running of the plant.

Connect

CitectHistorian connects people to information throughout the plant from multiple sources, including production control and business systems.

Reporting and analysis

Production data is transitory, changing state in real time rather than the hourly resolution with which business users are familiar. CitectHistorian captures and stores transitory data for reporting and analysis.

Present

Whether you need to analyze your productivity information in a spreadsheet or distribute it across the Internet, CitectHistorian produces accurate historical reports visible through your web browser, exportable to Microsoft Excel, Word or in PDF format.

CitectHistorian vs. Proprietary

	CitectHistorian		Proprietary Solution	
Total Cost of Ownership	✓	Low	✗	High
Complexity	✓	Low	✗	High
Openness	✓	High - Microsoft SQL Server	✗	Variable
Integration with other systems	✓	Easy and minimal cost	✗	Difficult and costly
Upgradability	✓	With Gold level support contract	✗	Not easily available
Scalability	✓	Easy	✗	Limited
Training required	✓	Minimal	✗	Time consuming and costly

What is CitectHistorian?

Historian

CitectHistorian provides an integrated long-term data archiving mechanism designed to store information from multiple disparate SCADA systems. The data store is an embedded Microsoft SQL Server 2008 R2 and can persist thousands of changes per second to the database (depending on hardware and configuration).

A relational database is well understood by both IT and production staff. It can be easily secured to control access to the historian data based on user security and is likely to be similar to existing systems on site. It reduces the friction between groups and the amount of maintenance or in-house knowledge that needs to be retained.

The historian collects all changes in the process tag values, as well as alarm activity, from each control system. Each change is saved with a timestamp and quality stamp.

The historian supports redundant control system links. In the event that one link fails, the historian will request the data from the other link to the control system. In the event that the network link to the historian fails, the historian will backfill from the control system's trend and alarm systems to acquire data that it could not acquire in real time.

The historian compresses data by saving only changes in values. For each tag, a deadband is available that will enable small ripples or insignificant changes to be filtered from the data that is stored. To calculate the exact disk requirements, CitectHistorian provides performance counters that show the number of changes that occur per second and the number of samples logged per second to the database.

The historian leverages the security of SQL Server to enable the user to secure each table, view and function within SQL Server.

The advantages of storing data directly in a SQL Server are evident when accessing the data from external applications. The large number of applications that have SQL connectors assists in making sure your data will be available in most of the applications that you require.

Configuration

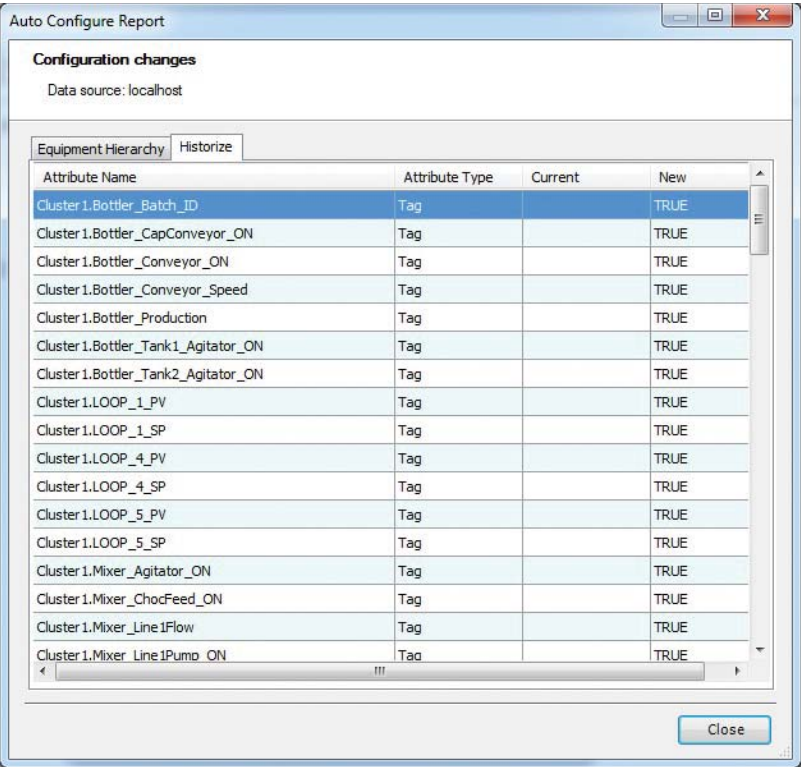
Setting up your historian has never been easier. CitectHistorian integrates with your CitectSCADA system to automatically configure itself with the tags, trends and alarms that were identified for historization when setting up your SCADA system. It organizes these tags by historizing and publishing them in the same equipment hierarchy already set up in SCADA, even further simplifying initial configuration.

As your SCADA system evolves, you can synchronize changes either manually or programmatically to ensure that your historian is always up to date.

For OPC® data sources, the same simple drag-and-drop interfaces are still available to help you arrange your data the way that you like it.

Data logging

Connections to CitectSCADA control systems are made through the CitectSCADA interface CtApi, polling at a rate that is defined at each data source. CitectHistorian acquires data from external SCADA systems via OPC V2 and OPC V3 Servers by subscribing to each tag and storing the changes. Data is stored in the database, along with meta-data describing the individual tag properties and quality for each sample.



CitectHistorian can be set to automatically configure itself with the tags, trends and alarms that were identified for historization when setting up your CitectSCADA system. When Automatic Configuration is run, a report of the changes that will be reflected in the Historian will be displayed

High performance

Reliability

CitectHistorian supports redundant connections to SCADA servers, with typical failover times of less than one second. In addition, if the historian is stopped, or there is a network failure between the historian and the SCADA servers, data is automatically backfilled from the SCADA trend system, if configured, enabling data continuity and quality.

Information any time, anywhere

Making data available to the right people anywhere and at any time is not simply about placing data within the database. It's about exposing the data in the correct clients and format for the user to be able to easily access and understand.

The CitectHistorian client for Microsoft Excel provides engineers and operations managers with the calculation tools they need to model and analyze production.

With a simple and intuitive interface, the client is designed to take full advantage of the advanced features of Excel to quickly and easily filter, sort, and analyze your historian data.

With historian now organised with a rich equipment hierarchy, the user can browse and filter published tags and create multiple profiles of data in Excel to easily capture comparisons between shifts, days weeks, batches etc.

The Historian Web Client provides maintenance engineers with a fast way to analyze trend and event data. The Web Client is a flexible means for them to compare real-time and historical data within one interface.

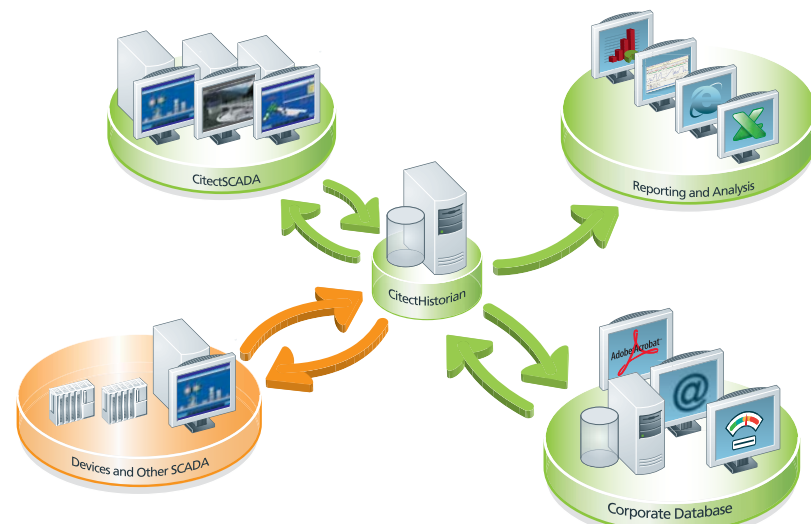
Managers often prefer their data to be presented graphically, with the ability to drill down for more detail into any results that may appear to be out of the ordinary. By utilizing Microsoft Reporting Services, they get a high quality reporting system that allows them to also customize reports for any of their process application.

Fast return on investment

CitectHistorian is a low-risk, low capital investment, open system that is easy to configure and maintain. It is a key enabler of operations optimization, and by leveraging and supporting common Microsoft technologies, return on investment can be realized in a short amount of time.

Optimize operational performance

CitectHistorian offers powerful performance with high data integrity, fast active data transfer rates and changes per second and unrivalled functionality — helping you get the data you want, in the format you want, when you want it. When used effectively, it becomes a key tool in the optimization of operational performance.



CitectHistorian architecture: Connect your production and business systems

CitectHistorian has allowed us to separate the reporting functionality from our SCADA system, and manage our reporting and control environments completely independently, thereby vastly reducing the level of manual intervention required for continuous customization of reports.

Stuart Henderson,
Process Systems Team Leader, Tomago Aluminium Australia

CitectHistorian Server

At a glance

CitectHistorian Server

- > Publishing data
- > Plant floor connections
- > Business system connections
- > Simple integration with other Schneider Electric products through EcoStruxure Web Services (EWS)
- > Logging data
- > Security control
- > Data transfers
- > ActiveX® scripts
- > High speed data acquisition and logging
- > OPC quality status and sub-status flags
- > Deadband compression

The CitectHistorian Server lets you decide what data you need without interfering with the running of the plant, and you don't need to be an expert in Microsoft SQL Server. CitectHistorian requires only a few mouse clicks to install, set up and view your data.

Configuration Manager

The CitectHistorian Server Manager is used to configure various aspects of CitectHistorian, including:

- > Plant control system connections
- > Database connections
- > Viewable (published) data
- > Security access
- > Tasks
- > Events
- > Logged data (historian)

Plant floor connections

The CitectHistorian Server connects to one or more plant control systems. When connecting to CitectSCADA 7.30, the Historian will automatically configure the tags, trends and alarms, by historizing and publishing them.

Database connections

The CitectHistorian Server supports connections to both Microsoft SQL Server and Oracle® databases. Once the database data source is created, it will automatically load the table structure. You can then start using this database.

Two typical requirements include:

- > Data archiving
- > Plant control system connections integrating plant floor data with existing third-party applications or ERP systems

Microsoft SQL Server historian

CitectHistorian utilizes Microsoft SQL Server 2008 R2 as its embedded historical data store. This industry standard bridges the gap between plant and business systems through a common server which is well-known and trusted among IT professionals. Additionally, its open, industry-standard technology and trusted security integrate effortlessly into your business and, with Microsoft Office, lowers your total cost of ownership. The simple roll-out of familiar Microsoft SQL technology results in reduced installation costs and little or no training time and expense.

Enterprise Edition of SQL Server 2008 R2 is also supported. Users wishing to use the Enterprise Edition can also benefit from data compression. This not only helps to reduce the size of the database, but because compressed data is stored in fewer pages, queries read fewer pages from the disk. Tests have indicated approximately a 43% compression ratio on process data. Enterprise Edition is not shipped with CitectHistorian and needs to be purchased from a third party.

Using the power of Microsoft SQL Server, information from plant systems and business applications is interconnected to provide you with a single view of the enterprise using industry-standard reporting tools. You can share files, email PDFs or use the web portal. This enables personnel at all levels to see where changes could be made to improve operations.

Universal connectivity

OPC HDA Server

OPC HDA Server is offered as standard protocol for CitectHistorian, closing the gap between systems by freely connecting to Manufacturing Execution Systems (MES), such as Schneider Electric's Ampla™ product. This connectivity can help deliver a fully integrated solution, allowing you to benefit from the latest product and services innovations from a single provider.

OPC DA Client

CitectHistorian supports data acquisition from OPC DA Clients. OPC DA is an industry standard protocol that allows you to connect to any third-party SCADA system, so that your Historian can provide complete storage and analysis requirements.

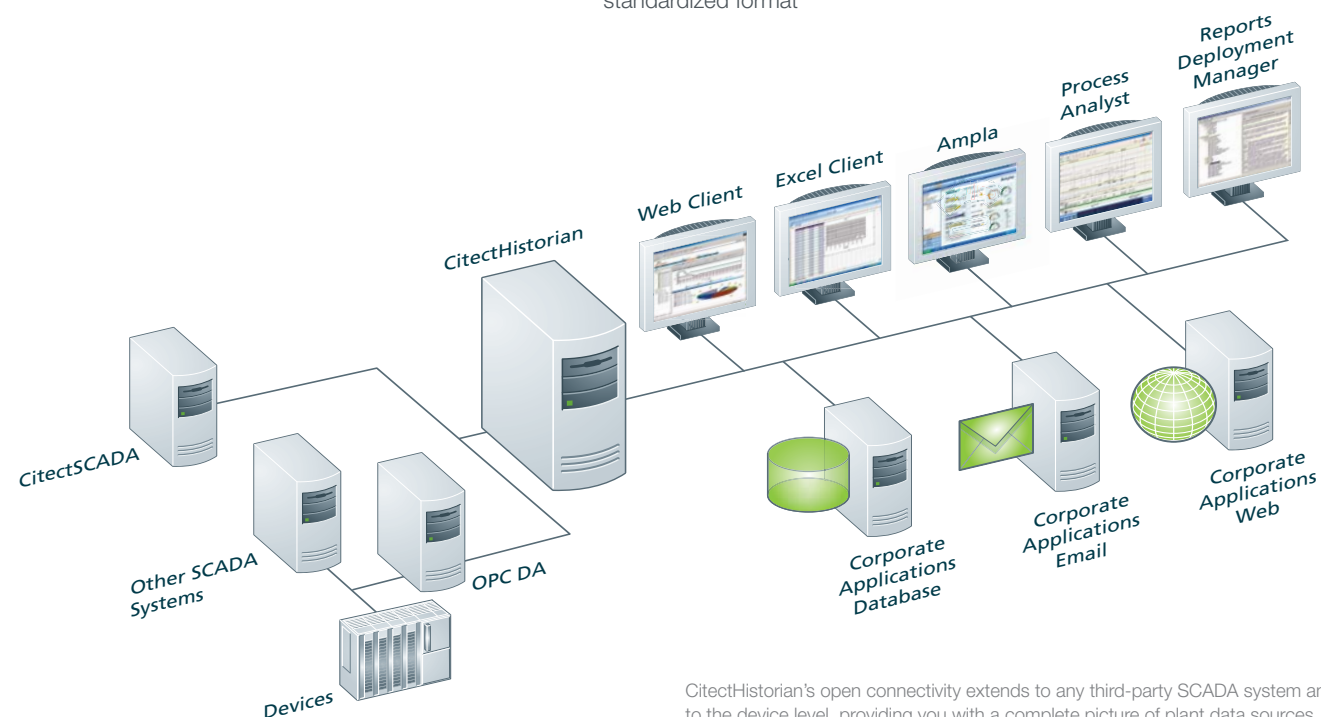
OPC DA Client is configured as a data source in CitectHistorian, which enables you to specify a redundant OPC Server per data source. The OPC DA data source connects to OPC DA V2 & V3 compliant devices, allowing you to obtain data from any SCADA system.

Seamlessly Connect Production and Business Systems

CitectHistorian is one of the industry's most open historians, designed to help you improve plant operation and management. By using industry-standard protocols, this integrated decision analysis solution will help bridge the gap between production and business systems. Consequently, companies are better able to analyze performance and more effectively manage ever-changing market demands.

This open architecture allows you to extract maximum value from the huge volumes of process data and realize benefits such as:

- > Reduction in project engineering costs and implementation times, with an improved interface that enhances visibility
- > Reduction in maintenance costs, with one standardized connectivity platform replacing multiple project solutions
- > Reduction in the load on systems, enhancing asset optimization
- > Assists in achievement of compliance with industry standards via defined best practice implementation processes
- > Fully integrated systems, with plant and corporate data more readily combined and available, enabling timely business decisions
- > Freedom to access manufacturing system data through a single point to business applications
- > Secure, long-term storage of data in a standardized format



CitectHistorian's open connectivity extends to any third-party SCADA system and even to the device level, providing you with a complete picture of plant data sources.



Historian architecture

Configuration data

Configuration data is stored in a Microsoft SQL 2008 R2 database. The configuration manager creates a registration to this database, and reads and writes the configuration data to and from this database. The Backup and Restore utility can be used to manage the storage of all configuration data to a file for use at a later time. This is useful when upgrading, or to take a snapshot of the project for use later on.

Historical data

Historical data is collected from the SCADA and OPC production data and stored in the Microsoft SQL historian database when the historian data service is running. This database is separate from the configuration database and can therefore be run on a separate machine and maintained separately. There are two modes of data acquisition. The default is real-time acquisition, whereby the data source is polled every poll period (default setting: one second). If the variable's value has changed by more than the deadband, then a new sample with the data service's timestamp will be logged to the historian database.

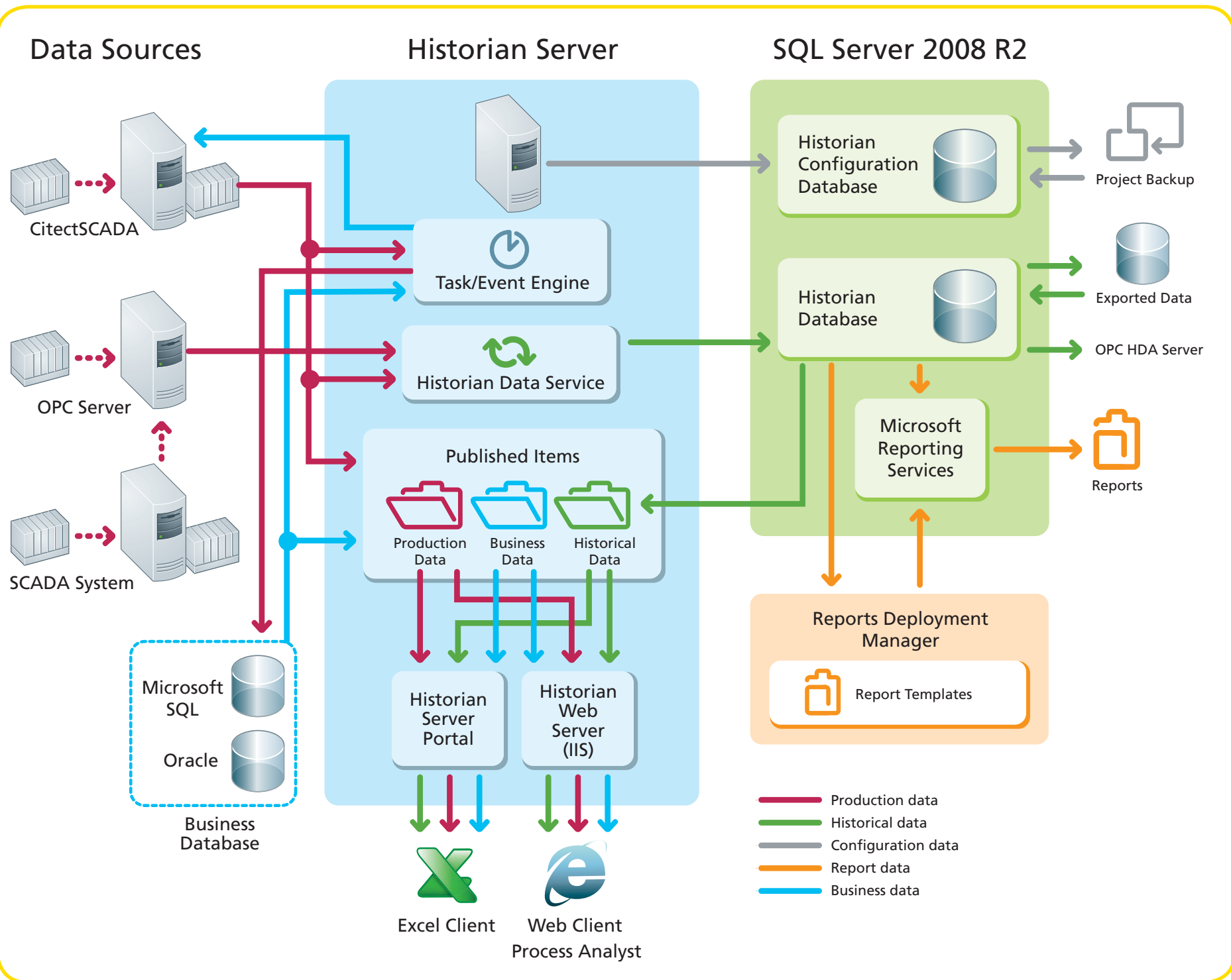
The other mode is trend data acquisition. This mode allows data collection from scheduled I/O devices such as Remote Terminal Units (RTU). However, it can also be used where it is preferable to request data from the trend server rather than from the SCADA system's I/O server. RTU devices periodically update the SCADA system with their data. In this mode, the historian data service requests the trend data from the SCADA system every 10 minutes by default. If there are changes since the last known good sample, data from the trend system is logged to the historian database. This mode only applies to SCADA data sources and not to OPC data sources.

Alarm data is requested by default every five minutes and changes will be logged to the historian database.

OPC data sources have an update rate which can be set per data source or per tag. This is similar to the poll period for SCADA data sources. However, since OPC uses a "publish and subscribe" model, it sets the minimum period in which the historian data service is notified of changes.

Report data

Reports in historian use Microsoft Reporting Services, a standard component of Microsoft SQL Server. The Reports Deployment Manager is an application in the historian used to select the historian database, the data source for the reports. It also deploys the reports to the reporting database. Reporting services will manage the data retrieval, rendering, scheduling and delivery of the reports. The report templates available in this pack can be used to generate alarm and energy reports, as well as some standard and developer reports for more generic applications. All of these templates can be customized in Visual Studio® as required. Deployed reports can be viewed in the Reports Deployment Manager or via the Reporting Services Report Viewer.



Data analysis

Powerful reporting

Creating professional reports and delivering them to the correct people is simplified with CitectHistorian. It uses the graphical query builder and report generation capabilities of Microsoft Reporting Services to deliver drag-drop-and-click reporting of any historical data from the historian.

With CitectHistorian, you can produce a range of reports using a convenient built-in historian in the familiar, open Microsoft user interface which only an embedded Microsoft SQL server makes possible. The combination of the powerful reporting tool and Process Analyst makes it easier for you to make sense of the vast volumes of generated data. The reports can be built using stored procedures and (table value functions) that are defined within the historian database, or can be directly driven by the data in the historized tables.

The stored procedure interfaces enable the data, which is stored only when the data changes, to be returned as a set of time-series data (e.g. 30 second averages). The data can be based on raw values or by interpolating between recorded values.

The table value functions also process the raw data with a focus on enabling the data to be grouped. Reporting often requires the maximum of a variable during the production of a product or the total for a set of production runs, or even just the runtime for a device (or all devices) within the system.

These views allow the user to query statistical data, including maximum, minimum, average, total, count or on-time of any variables or conditions. These values can be grouped by time, the value of a tag (such as a batch ID), an event (such as a pump running) or by an alarm (allowing reports for the data preceding each occurrence of an alarm). Views can also provide an alarm summary and alarm event lists.

Reports are generated using Microsoft Reporting Services. By using an industry standard report generation tool, CitectHistorian reduces the cost of report development training. Reporting Services provides templates for report design, a drag-and-drop environment to extend the base reports and a full-featured reporting system compatible with every other major business.

Once generated, reports are deployed to the CitectHistorian server and scheduled to run based on an advanced scheduler. Scheduled reports can be sent to managers by email or recorded in a file share. In either case, the user is able to select to receive the report as HTML, PDF or an Excel spreadsheet. In this way, reporting data can act as a secure record or as a starting point for more detailed plant analysis.

Reports are also accessible via web browser. This enables them to be integrated into the CitectHistorian Web Client, CitectSCADA or any corporate reporting system.

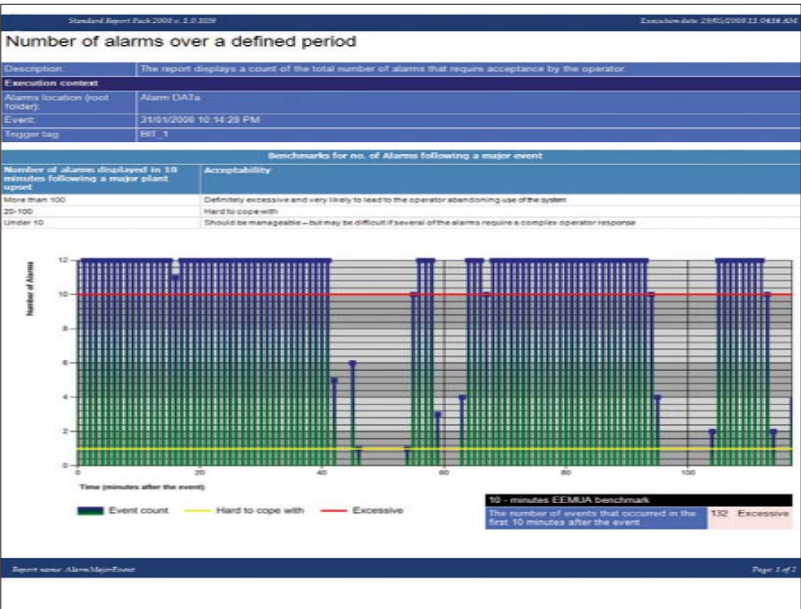
Reports are enhanced with advanced charting controls and gauges facilitated by Microsoft SQL Server 2008 R2.

Alarm rationalization and alarm management reports (EEMUA 191 guidelines)

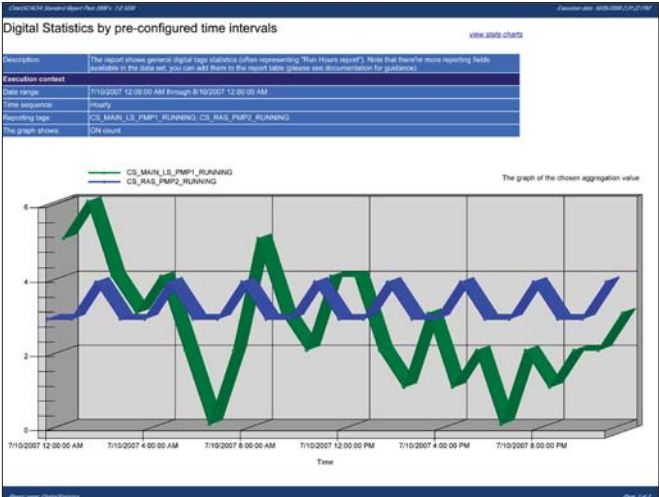
Alarm systems have long been an intrinsic part of plant safety management. They play a critical role in alerting operators to a change in operations at a process plant; inform operators about the nature of the change; and guide operators to implement corrective action.

Poor alarm management can result in:

- > Increased downtime
- > Reduced plant productivity
- > Reduced quality
- > Reduced operator effectiveness
- > In the worst-case scenario, serious industrial accidents
- > Increased insurance premiums on plant equipment or fines



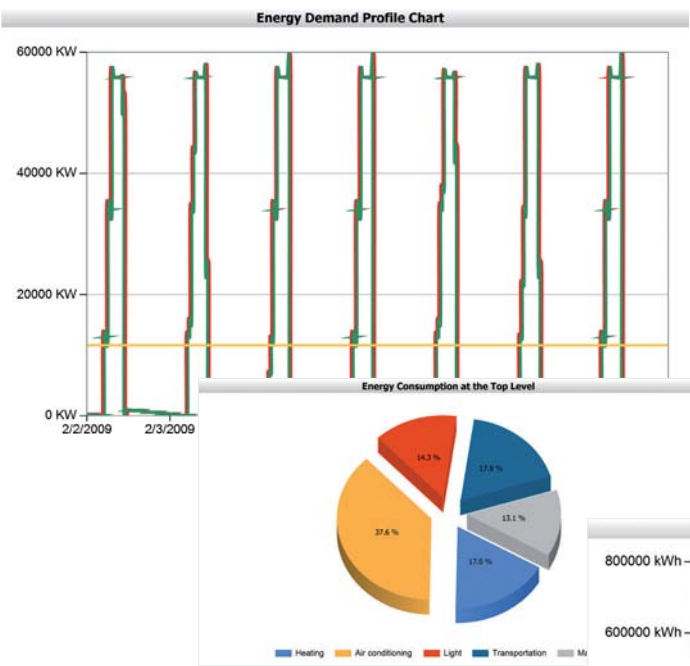
Out-of-the-box alarm rationalization reports based on EEMUA 191 guidelines.



CitectHistorian, the plant-wide reporting tool, is capable of accurately recording all alarm data and tag values at high speed. Such a tool can help engineers and operators gather and organize alarm data from across their entire site.

Alarm management is a set of procedures, practices, tools and systems that jointly assist in making sure a plant's alarm system is effective throughout the life of the plant. CitectHistorian provides pre-configured alarm rationalization reports based on the EEMUA (Engineering Equipment & Materials Users Association) 191 alarm management guidelines.

With alarm management reports, operators are provided with more meaningful and actionable information. The reports are designed to improve the average and maximum number of alarms per hour, operator response times, usability and relevance.



Comparison matrix (by groupings)		Feb 02, 09 - Feb 09, 09			Feb 09, 09		
		Energy	Avg Power	Peak Meter Power	Energy	Avg Power	Peak Meter Power
Light	PowerMeter55	30.24 MWh	180.00 kW	252.00 kW	17.28 MWh	102.86 kW	102.00 kW
	PowerMeter59	28.22 MWh	168.00 kW	240.00 kW	16.13 MWh	96.00 kW	96.00 kW
	PowerMeter60	15.12 MWh	90.00 kW	126.00 kW	8.64 MWh	51.43 kW	51.43 kW
	PowerMeter54	7.06 MWh	42.00 kW	60.00 kW	4.03 MWh	24.00 kW	24.00 kW
	Total	80.64 MWh	480.00 kW	252.00 kW	46.08 MWh	274.29 kW	274.29 kW
Heating	PowerMeter51	22.18 MWh	132.00 kW	204.00 kW	13.11 MWh	78.06 kW	78.06 kW
	PowerMeter52	12.10 MWh	72.00 kW	108.00 kW	7.35 MWh	43.77 kW	43.77 kW
	Total	34.27 MWh	204.00 kW	204.00 kW	20.47 MWh	121.83 kW	121.83 kW
Transportation	PowerMeter56	11.09 MWh	66.00 kW	102.00 kW	6.34 MWh	37.71 kW	102.00 kW
	Total	11.09 MWh	66.00 kW	102.00 kW	6.34 MWh	37.71 kW	102.00 kW
Air conditioning	PowerMeter53	8.74 MWh	52.00 kW	76.00 kW	5.43 MWh	32.35 kW	1.80 MW
	Total	8.74 MWh	52.00 kW	76.00 kW	5.43 MWh	32.35 kW	1.80 MW
Machinery	PowerMeter57	8.06 MWh	48.00 kW	72.00 kW	4.61 MWh	27.43 kW	72.00 kW
	Total	8.06 MWh	48.00 kW	72.00 kW	4.61 MWh	27.43 kW	72.00 kW
Total		142.80 MWh	860.00 kW	252.00 kW	82.93 MWh	493.61 kW	5.36 MW

CitectHistorian centralizes the data for energy usage and provides analysis tools to easily identify the causes of excess energy consumption or peak demand in real time.

Comprehensive energy reports to manage energy

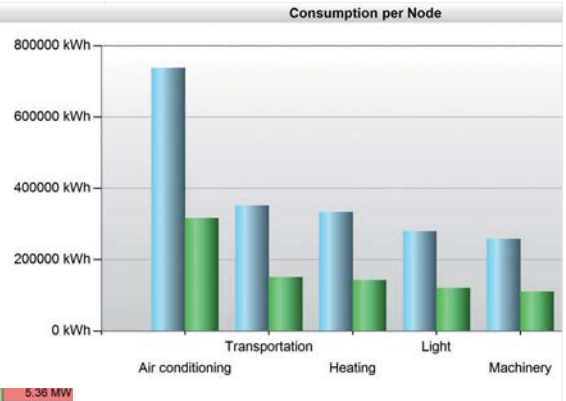
Schneider Electric's Energy Management offer delivers a unique and effective approach to energy efficiency, connecting automation and control with energy monitoring to optimize energy consumption. By delivering reliable, accurate energy consumption data in context with production variables, customers gain insight into the efficiency of the operating environment while effectively removing energy waste in the process.

Today's plant historians can play a key role in energy management initiatives. By capturing energy-related information, users can better understand energy usage over time and have a way to gauge whether agreed energy management procedures are being followed.

Plant historians can be used to identify inefficient plant equipment or processes, diagnose unexpected anomalies in power usage and make real-time adjustments to optimize energy efficiency and save costs.

CitectHistorian comes with ready-to-use energy reports that can facilitate energy consumption assessment and potential savings across the equipment level, production lines, an entire plant or multiple sites.

The historian centralizes the data for energy usage and provides analysis tools to easily identify the cause of excess energy consumption or peak demand in real time. A simple analysis of consumption over the past five days, the past five Mondays or the equivalent day in the previous year could provide valuable clues to the causes of changes in energy consumption. Also, by overlaying different time periods, changes in consumption become easily apparent.



At a glance

- Citect-Historian is designed for high performance, long-term data archiving:
- > Engineering value precision
 - > OPC quality flags
 - > Sub-second acquisition rate
 - > Sub-second failover rates
 - > Backfilling capabilities
 - > Client access through Citect-Historian Server

Reporting data sources

- > Citect-Historian
- > SQL Server
- > OLE-DB
- > ODBC
- > Oracle
- > Web Services

Reporting output formats

- > HTML
- > PDF
- > Excel

Reporting delivery

- > Email
- > File Share
- > Web portal

With Microsoft Reporting Services and Office integration providing additional tools

Meeting regulatory requirements

For data analysis to be valid, you need to first be able to trust it. The historian data collection is critical to your ability to have confidence in the results. The data collected in CitectHistorian includes any tags within the control system, alarms and events from SCADA systems and event or tag comments on any recorded data, resulting in a rich source of information for data analysis.

By using data from your control system or connecting directly to external data sources, CitectHistorian can store the complete picture and manage it for quality and regulatory requirements.

Reports Deployment Manager and Standard Sample Reports Pack

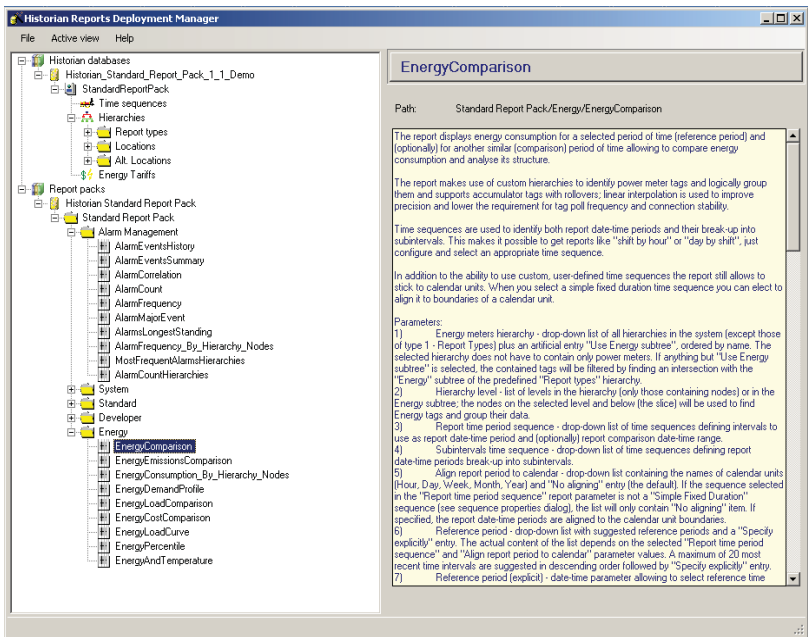
The Reports Deployment Manager delivers a standard set of pre-configured reports. Its out-of-the-box sample reports contain a collection of reports designed to meet the needs of specific industries or skill levels, simplifying alarm and tag reporting.

- > Standard reports
- > Developer reports
- > System reports
- > Energy reports
- > Alarm rationalization and alarm management reports (based on EEMUA191 guidelines)

Alternatively, you can opt to customize these reports to suit your individual requirements. We have introduced the concept of hierarchical tag grouping. Enables you to organize the data according to your business reporting requirements.

The Reports Deployment Manager is the application used to manage and implement report packages. It will:

- > Connect to CitectHistorian database
- > Install a standard sample report pack, including the new energy reports, on CitectHistorian
- > Deploy reports in Microsoft Reporting Services
- > Manage client access to deployed reports



Energy Comparison report available through Reports Deployment Manager

Process Analyst

Turning data into meaningful information

Process Analyst is an intuitive visualization tool that allows operators and process engineers to analyze the cause of process disturbances by bringing together trend and alarm data which are traditionally stored separately. With Process Analyst, a standard feature in CitectHistorian, users can simply view this data on a single integrated display.

The user is given complete flexibility with regards to the ways in which the pens can be displayed. For example, they can be overlaid or stacked or even moved to different panes to reduce clutter and make the display simpler and easier to read.

Process Analyst includes many unique features including true Daylight Savings Time support, accuracy to millisecond resolution, individual time axis per pen, customizable toolbars, rich printing and saving of display settings for easy recall.

Process Analyst helps to:

- > Identify any 'process drift' towards an abnormality which could eventually lead to breakdown or process failure
- > Link alarm spikes to specific process conditions, changes in instrumentation or new or changed control system configurations
- > Analyze operator responses to alarms as a means of detecting poor alarm system design
- > Isolate consequential/source alarms, as well as nuisance alarms

Examples of use

Root cause analysis

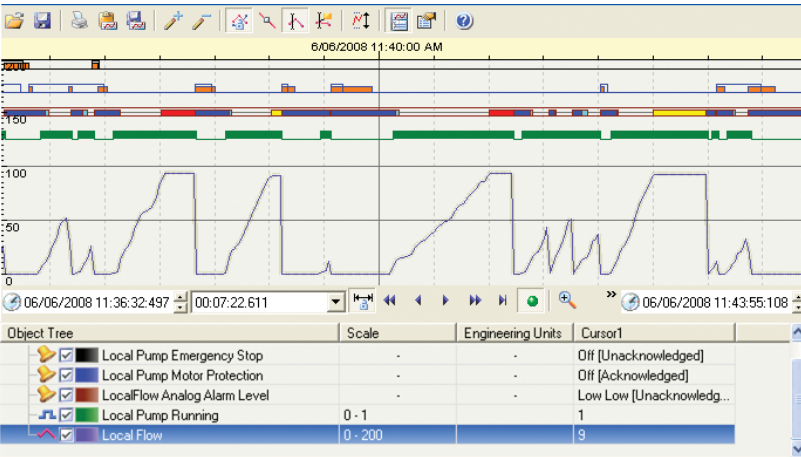
When a process upset or disturbance occurs, finding the root cause is always time consuming. In the past, the process engineer had to compare trend data from the screen with alarm logs. With Process Analyst, the engineer simply needs to add to the display any pen (analog, digital, alarm) that could have contributed to the process upset. Each process change can then be easily compared as alarms occur, enabling sophisticated analysis of the process upset.

Compare different batches

With Process Analyst, it is easy to compare different batches in a single integrated view. Simply place the variable tags, alarms and state changes for a batch unit on one pane, and the same set on a separate pane. Then, the operator simply has to scroll one of the panes through time. Any differences in the batch execution will immediately become apparent.

Sequence of events

With large systems, the data can be distributed around a wide area and typically the RTUs collect the data at millisecond resolution. Process Analyst displays historical alarms and trends to millisecond accuracy, making it easy to determine the sequence of events.



Process Analyst: Get the complete picture with one viewer and improve productivity.

Improve operations with Process Analyst

At a glance

- > Analyzes the cause of process upsets quickly and simply
- > Allows operators to recognise patterns that may lead to process disturbances
- > Provides total flexibility on how you view and analyze your process
- > High quality output to printers
- > True Daylight Savings support

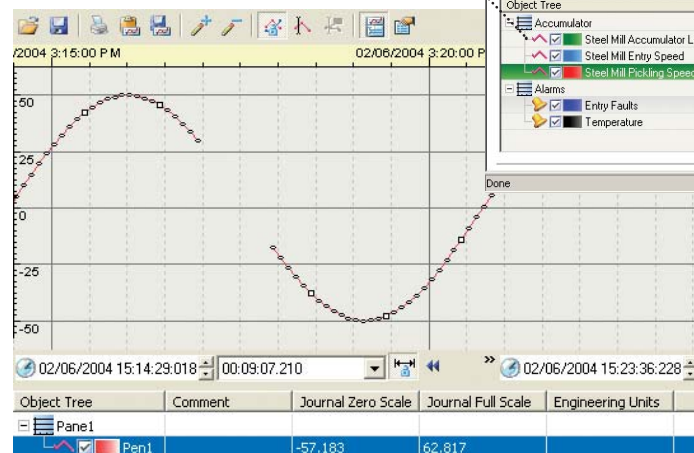
Save the current view as either a template or process snapshot

Individual pens can be unlocked, allowing their values to be compared in different time frames

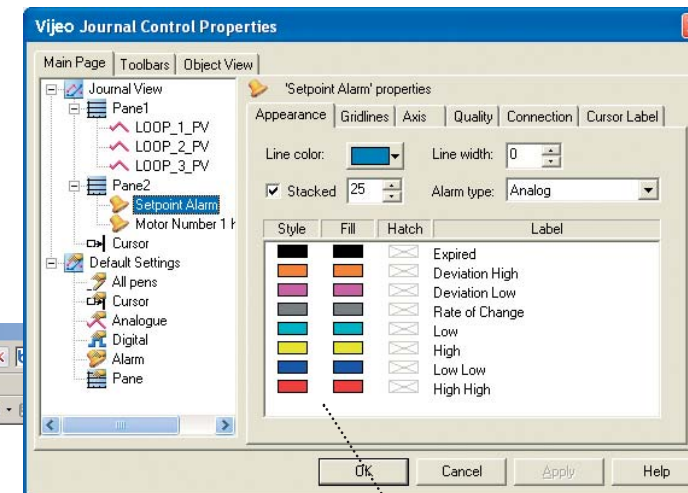
Multiple trend cursors can be displayed with or without tool tips

Overlaid analogue and stacked digital pens on the same pane

Operators can easily declutter the display



Trend example showing different quality attributes.



Alarm pens can represent different alarm states with colours or fill patterns

Alarms can be overlaid or displayed on a separate pane. The pen displays the ontime, offtime, acknowledge time, and operator comment

The value of any pen is displayed at the current cursor location

Easy to use

Process Analyst's capability to display such rich information requires it to have an easy-to-use, yet powerful navigation system. Every pen added to Process Analyst has a number of properties including:

- > Pen colour and name
- > Tag properties such as Engineering Units, Scales etc
- > Cursor values (multiple cursors are available)
- > Data average / minimum / maximum

The information available is customizable, allowing you to add or remove any of the standard column types (e.g. Engineering Units), as well as add custom columns.

Customizable

Users can select which buttons to appear on each instance of Process Analyst. The security access required can also be defined and users can add custom buttons for additional functionality.

Data exchange and integrity check

At a glance

- > Visualize data from multiple SCADA systems in the web browser
- > Ad hoc data analysis and simplified reporting with Excel
- > Analyze and understand the cause of process upsets and compare alarm and trend data to improve efficiency via intuitive visualization tool
- > Make sense of large volumes of tag-based data with easy-to-use reporting tools
- > Transfer data between your control systems and Microsoft SQL or Oracle databases
- > Historize control system data into Microsoft SQL Server 2008 R2
- > Report using industry standard reporting tools

Support for timestamped tag data

Typically, timestamped data is cached and pushed into a SCADA system after it has been acquired. This results in the loss of the original timestamping as the time polling takes precedence. CitectHistorian now includes a "historical" data acquisition method, that allows tag value changes to be timestamped in your historian database. Using this historical mode, data is acquired based on the last read sample time for each timestamped tag.

Support for clustered SCADA systems

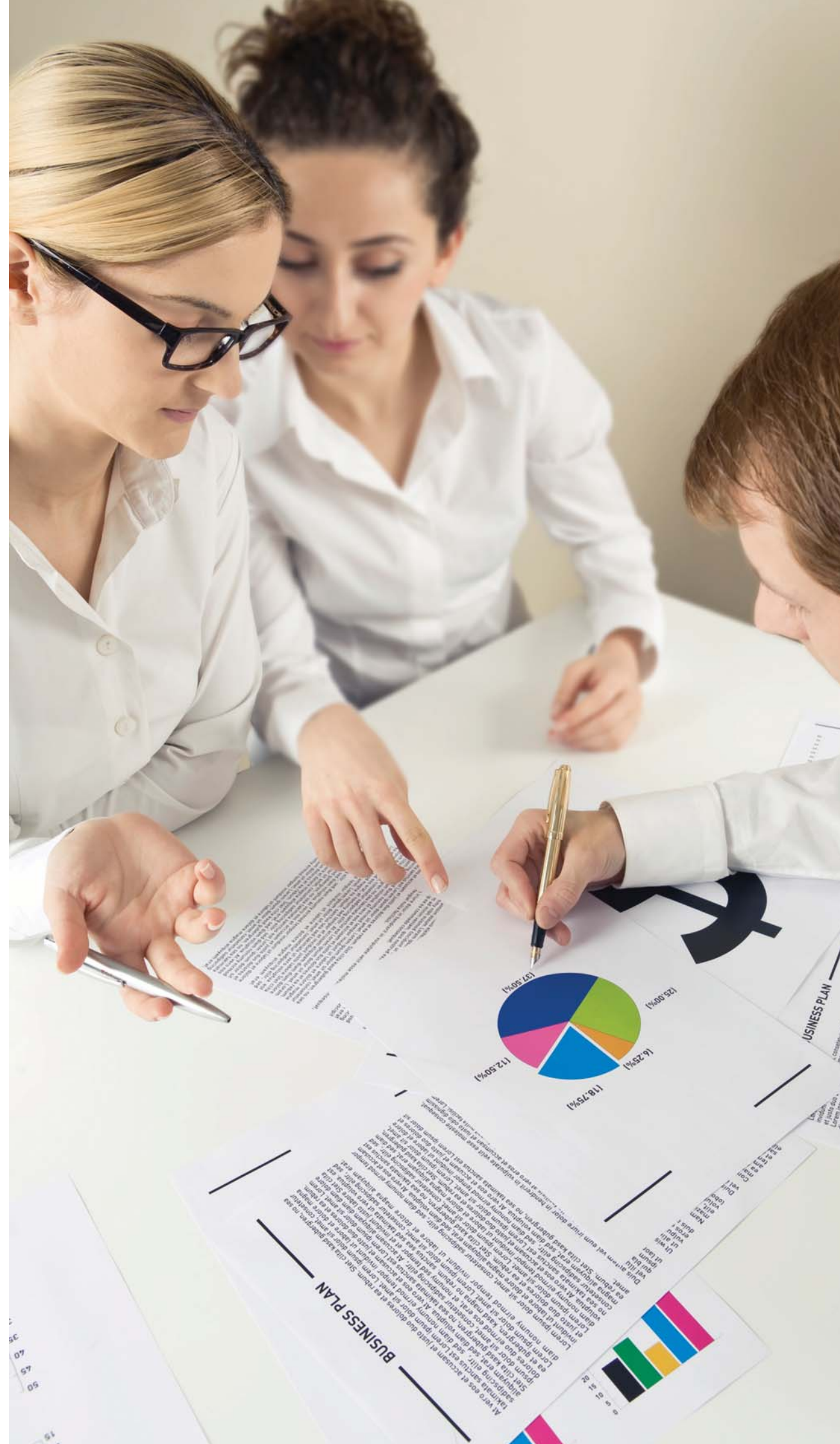
Clustering refers to the grouping of server components within a single SCADA project, allowing multiple systems to be monitored and controlled. CitectHistorian will automatically detect a clustered system and indicate the number of clusters identified. Once CitectHistorian's Configuration Manager is populated with the data from a clustered system, the detected clusters appear as an additional level in the data hierarchy.

Integrity Checker

The Integrity Checker is an embedded tool that helps you verify there are no unbound SCADA attributes (variable tags, alarms and trends) located in the Published Information and Historian folders. It can be activated at any time and can also be used to check all configured tasks, events and trends under a data source node. If unbound attributes are found, the tool allows you to restore bindings on an individual or grouped basis.

Security

To allow only authorized access to the published information on the CitectHistorian Server, it is important to define who can access plant and business data and what permissions they have. It is also important that CitectHistorian sits in a secure environment in order to provide a high level of security. User access to individual data items, published folders and user Favorites can be restricted to individuals or groups.



Requirements for CitectHistorian 4.40 Server

- > 5GB disk space for full installation or 211MB without SQLServer
- > 2.4 GHz, Dual-Core Processor
- > 4GB (DDR 2) RAM
- > TCP/IP network connection (must be active)
- > SATA 1 disk speed (1.5Gb/s) 7200 RPM Drive

Recommended (15000pt Historian)

- > 2.4 GHz, Quad-Core Processor
- > x64 Operating System for faster RAM transfers and expansion of memory later
- > 8GB (DDR 2) RAM
- > TCP/IP network connection (must be active)
- > SATA 1 disk speed (1.5Gb/s) 7200 RPM Drive

Supported Connectors

- > CitectSCADA V7.0 or later, CitectHMI V7.0 or later, Microsoft SQL 2008 R2

Pre-load software requirements for CitectHistorian 4.40 Server

- > Microsoft Windows Server® 2003 (SP1), Windows XP (SP3), Microsoft Windows Server 2008 R2, or Window 7
- > Microsoft Internet Information Services (IIS)
- > Microsoft Message Queue (MSMQ without active directory)
- > Microsoft networking or loopback adapter
- > Internet Explorer® 6 SP1 or later
- > Updates need to be installed for the above components and operating systems

Flexible configuration

The following CitectHistorian components can be installed on the same OR separate PCs:

- > Citect-Historian Configuration Manager
- > Process Analyst
- > Microsoft Excel Clients
- > Citect-Historian Web Clients
- > Reports Deployment Manager
- > Historian Database

The following CitectHistorian components must be installed on the same computer:

- > Citect-Historian Server
- > Citect-Historian Web Server / Client
- > Citect-Historian Configuration Database
- > Configuration Manager

Aliases can be assigned to make production identities more applicable to the information domain. Access item properties to change name, permissions etc.

View Favorites that are currently open with a single click.

User who is currently logged on.

Data Sources include plant control systems and OPC servers' database connections.

Create folders here to organize historical Tags. Drag and drop data items from the SCADA and OPC data sources into these folders.

Citect-Historian Web Client Favorites for all users are stored in this folder.

Create folders here to store published information. Simply drag and drop data items from the data sources and historian node into these folders.

Events can be either scheduled or trigger-based.

Tasks perform actions such as data transfers or running ActiveX scripts.

Only displays the items the logged-on user has permission to view.

The Summary window displays the data items for this Favorite.

This window displays the parameters for the currently selected data item.

Window for displaying time series data. Example shown is a histogram.

Window for displaying events and alarms. Example shown is a Pareto chart.

Window for displaying snapshot data. Example shown is a data list.

Name	Description	Type	Source
Cluster1.digital1	Digital Alarm 1	SCADA Alarm	Cluster1.digital1
Cluster1.digital2	Digital Alarm 2	SCADA Alarm	Cluster1.digital2
Cluster2.digital1	Digital Alarm 1	SCADA Alarm	Cluster2.digital1
Cluster2.digital2	Digital Alarm 2	SCADA Alarm	Cluster2.digital2
Cluster3.digital1	Digital Alarm 1	SCADA Alarm	Cluster3.digital1
Cluster3.digital2	Digital Alarm 2	SCADA Alarm	Cluster3.digital2
Cluster4.digital1	Digital Alarm 1	SCADA Alarm	Cluster4.digital1
Cluster4.digital2	Digital Alarm 2	SCADA Alarm	Cluster4.digital2

TimeSeries	Cluster1 Entry	Cluster1 Entry	Cluster1 Entry
22/09/2009 4:44:59 PM	1527	2317	8047
22/09/2009 4:46:08 PM	2147	2459	6049

The Citect-Historian Configuration Manager is the tool used to turn plant floor data into useful information.

Five simple steps to configure historical data in Citect-Historian:

1. Create Historian Data folders
2. Drag tags required to be stored in Citect-Historian from SCADA and OPC data sources into the Historian Data folders and start the historian service
3. Create Published Information Data folders
4. Drag the historical data required to be viewed by clients from the Historian Data folders into the Published Information Data folders
5. Define the security on the published data

Data access via Web and Excel Clients

Applications

- > Information anywhere any time – visualize and analyze plant floor information from anywhere within the entire plant or over the Internet
- > Plant-wide reporting – generate consolidated reports that include both plant floor and business information

CitectHistorian interfaces:

- > SQL Native Client
- > OLE-DB
- > ODBC
- > OPC HDA Server
- > OPC DA Client V2.05, V3.0
- > EWS

Historian performance Historian Poll

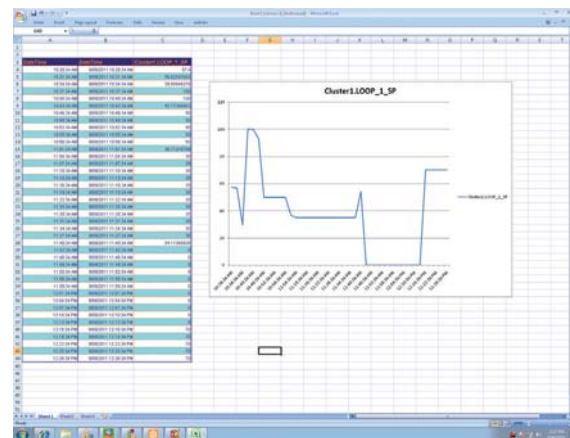
- > 100ns (or greater)
- > Deadbands (per tag)

Historian Data Accuracy

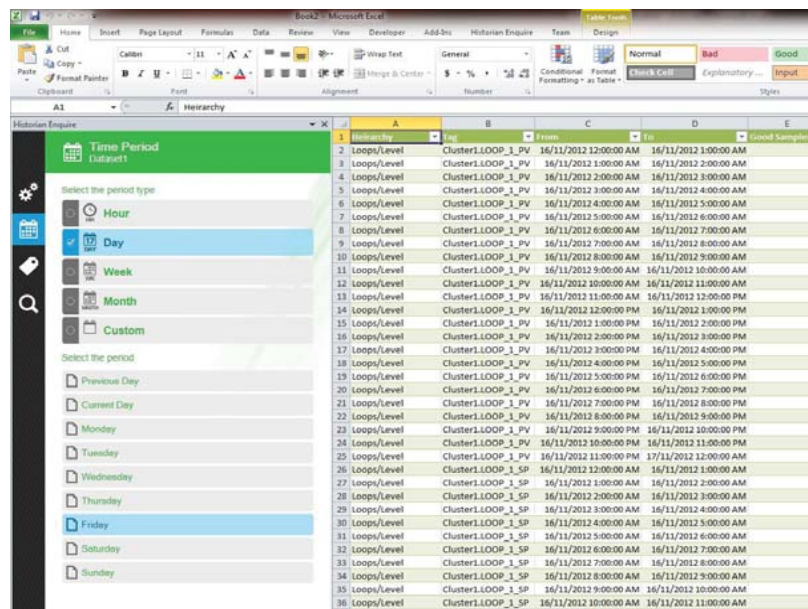
- > 1ns (for external timestamped data)
- > OPC Quality Flags

Historian Security

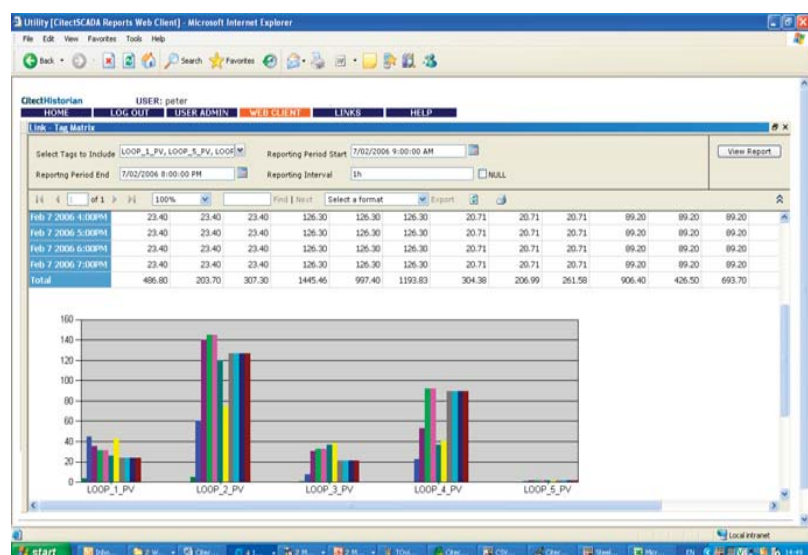
- > Windows Integrated or SQL user-based
- > Secure each table, item, procedure



CitectHistorian graph display



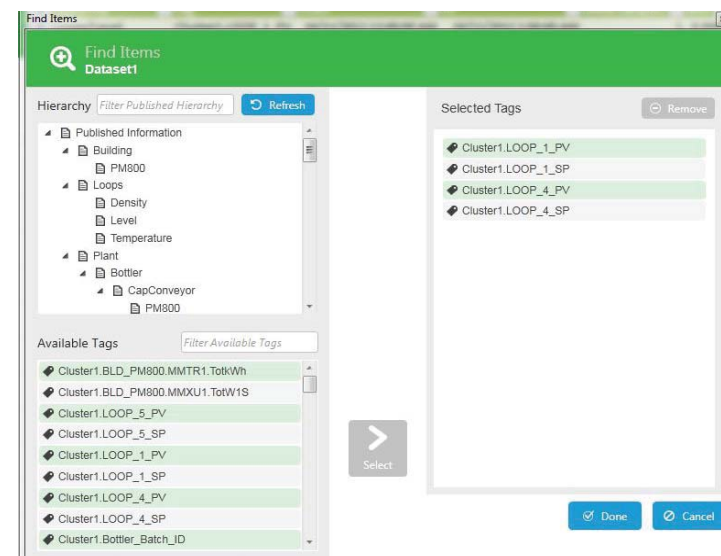
Historian Client for Microsoft Excel, Historian Enquire



Data display



CitectHistorian Web Client includes a powerful built-in alarm analyze



Using configuration datasets that are now stored in a configuration table in Excel, users can create datasets for specific periods

Favorites

In CitectHistorian Web Client, user Favorites can be created simply by double-clicking on any published data item or dragging and dropping it into the Summary window. Favorites can then be saved on the CitectHistorian Server.

Security

To use the CitectHistorian Web Client, you need to first log on.

Once logged on, you can only access the published folders, data and Favorites that you have permission for.

Historian systems, like any other business system, need to be protected from unauthorized access. It is highly recommended that a secure Internet connection, such as a Virtual Private Network (VPN), firewalls and intrusion detection systems are used in order to prevent outside access to your network while you are connected over the Internet.

Web links

CitectHistorian can link directly to external websites, providing an organized structure for rapidly accessing relevant sites and information. For example, CitectHistorian information can be co-located with other pertinent intranet pages and accessed through the CitectHistorian web portal.

Additionally, you can leverage the built-in security and user validation provided in the CitectHistorian Web Client by incorporating custom .ASP pages into the tree hierarchy and security model.

Data access

The data made available by CitectHistorian is customizable to suit individual process needs. Each data item can be named appropriately for business users and located (independent of its data source) anywhere within a free-format tree structure to represent your plant or process. The available areas of this tree user can be filtered to provide users with the exact information they require.

This tree structure is used throughout CitectHistorian clients. In Excel and Web Clients, the tree enables users to easily find the data they need. The location of a device or tag within the structure can be used in a parameter to allow dynamic reporting.

Web and Excel Clients

Using CitectHistorian Web Client, you can visualize plant information from your control systems and historian over an intranet simply by using Internet Explorer. Built-in views include time-series line and XY graphs for analyzing analog values over time, Gantt charts for analyzing state changes over time, Pareto charts for analyzing frequency and duration of states, as well as data lists which allow raw plant data to be pasted directly from the web browser into other applications. The Web Client analytical tools can also be used on real-time tags to take snapshots of current values and display them as a real-time trend.

The CitectHistorian Web Client can also act as a portal to the reports generated by the reporting system. Web pages can also be integrated and viewed within the CitectHistorian hierarchy.

Optimize your investment in SCADA, MES and Historian technologies

Gold

Direct Access Support

Fast access via telephone, live chat, e-mail and Case Manager during normal business hours* to experienced Support Engineer professionals supported by a comprehensive lab where they can replicate a customer's configuration and reproduce issues experienced onsite.

Online Support Tools

A dedicated area of the SCADA & MES Support website (www.citect.schneider-electric.com) gives you access to a range of support tools including: Case Manager, Live Chat, Toolbox, DriverWeb, Driver Discussion Forum, Authorization Code Generator.

Product Upgrades

SCADA & MES Software Global Support will provide notification of new releases and product upgrades (available for download). Support can assist and advise on appropriate planning and risk mitigation.

Driver Upgrades

Automatic product updates keep you at the forefront of technological advancements in drivers (available for download).

Service Packs

Support customers are advised of new service packs and are provided with links to download.

Emergency Support

Emergency software patches are provided via an intensified escalation process in situations where critical issues are impacting upon customer business operations.

Customer Service Request (CSR) Resolution Workflow

A rigid framework of issue prioritization and severity ensures an appropriate management process is applied to all your issues until resolution. Prioritization is based on industry best practice.

Online Knowledge Base (KB)

Support customers can access the KB anytime for information that consistently delivers support services and resources to sustain customers' return on investment.

Security Advisory Service

Users may subscribe to the Knowledge Base (KB) under Security to receive RSS feeds whenever the KB is updated. SCADA & MES Software Global Support will provide proactive notification for any known Security issues that affect the Product, allowing customers to take immediate action to protect their systems.

The Insider Newsletter

Your source for the latest Support updates, new product information, technical tips and tools, The Insider is a quarterly newsletter distributed exclusively to customers in support.

GoldPlus (all the above features plus)

Priority Telephone Support

24/7 priority access to the Support service via a dedicated telephone access point, minimizing the response process and optimizing resolution times. The service offers engineer call-outs at preferential rates..

Priority After Hours Telephone Response Commitment

Assurance of a 15-minute response commitment on calls placed 24/7.

Priority Customer Service Request (CSR) Resolution Workflow

Support calls not progressed within 15 minutes for critical severity issues by the first line support engineer are automatically escalated to a Senior Support Engineer. Support calls not progressed within one day for major and medium severity issues by the first line support engineer are escalated automatically to a Senior Support Engineer.

Optional Support Services (subject to additional fees)

Enterprise Support

Global Enterprise Support Agreements can be set up to include any of SCADA & MES Software Global Support services. An Enterprise Support Agreement ensures a single point of management, common commercial terms and annual purchasing price reviews. Multiple global sites are covered and additional sites can be covered at any time during the Support Agreement, subject to a fee.

Specialty Driver Support

Specialty Driver Support is an add-on support service to Gold and GoldPlus Support agreements. Specialty Driver Support is required for the following licensed drivers: Bailey, IEC870-5-104, Moscad and SemAPI.

Service Capability & Performance (SCP)

The SCADA & MES Software Global Support organization is SCP certified so you can be assured of quality service. SCP certification quantifies the effectiveness of customer support based upon a stringent set of performance standards and represents best practices in the industry.

Support Services

A range of direct and self-help technical assistance options allows you to maintain optimum performance from your software, whilst automatic product updates keep you at the forefront of technological advancements.

Maintenance and Support Agreements cover all our software, as well as Standard Drivers. Specialty Driver Support is required for the following licensed Drivers: Bailey, IEC870-5-104, Moscad and SemAPI. Specialty Driver Support is an add-on support service to Gold and GoldPlus Support Agreements.

SCADA & MES Software Global Support

*Hours are 9am to 5pm, Monday to Friday, local time. Technical Support is provided in English only.

Customer Service Resolution

Optimize your technology investment with our SCADA & MES Software Global Support offering. Customers with maintenance and support agreements are entitled to receive product upgrades, service packs and hotfixes . In addition, you get access to our professional SCP-certified and trained support team who can help you overcome issues quickly and easily, either by phone, live chat or email. We also offer the option of 24/7 support with some of our support contracts.

Customer Service Requests (CSRs)

Our centralized SCADA & MES Software Global Support enables logged Customer Service Requests (CSRs) to follow the CSR Technical Resolution Workflow. A fully documented procedure, this model allows calls to follow a clear path to resolution, giving you updates at every stage. CSRs can be logged by telephone, Case Manager, live chat or email. The recent introduction of our Case Manager tool allows you to manage, update and monitor the progress of your CSRs via the Internet.

Virtual Engineer

Virtual Engineer allows one of our Support Engineers to securely connect to your system anywhere in the world and cost effectively locate the cause of your issue. Improved response and resolution times have been documented since the implementation of this industry standard authentication technology. This means your issues are dealt with quickly, minimizing any disruption to your business.

Additional Information

For Critical and Major severity cases, Account Managers and Support Management are informed of the case progression through the workflow. During case workflow, Support Developers and the Support Engineers may consult with the Product Development group and other resources.

Technical Resolution Workflow	Support Engineer	Senior Support Engineer	Support Developers
Critical severity* GoldPlus customers	15 Minutes	Not able to be progressed within 1 business day and product defect suspected	Cases scheduled based on severity model**
Major & Medium severity* GoldPlus customers	Not able to be progressed within 1 day	Not able to be progressed within 3 business days and product defect suspected	Cases scheduled based on severity model**
Critical severity* Gold customers	Not able to be progressed in 2 hours	Not able to be progressed within 2 business days and product defect suspected	Cases scheduled based on severity model
Major & Medium severity* Gold customers	Not able to be progressed within 3 business days	Not able to be progressed within 4 business days and product defect suspected	Cases scheduled based on severity model

*Schneider Electric will determine the severity of an issue by analysis of the impact and urgency of a reported issue.
**GoldPlus customers receive additional priority in scheduling.

Educational Services

Educational Services offer a suite of programs and courses designed for end users, engineers, system integrators, technical colleges, universities and educational establishments.

Our courses provide you with hands-on experience, leaving you feeling confident to design and configure your own systems whilst our programs are designed to facilitate the latest education and application of our software. Instructor-led, online, onsite and self-paced courses are offered. Courses include configuration and programming courses, update courses and introductory courses for CitectSCADA and CitectHistorian.

Programs include the Certified Education Centre Program which regulates the standard of our courses. The Academic Program provides tertiary institutions with access to world class courseware to use in conjunction with their degree and diploma courses in related fields. The Certified Engineer Program (CEP) recognises engineers skilled in the integration of automation projects using our software. The first of these qualifications is the CitectSCADA Certified Professional (CSCP). To gain this qualification, an engineer or operator needs to pass the SCADA Configuration exam. To become a CitectSCADA Certified Engineer (CSCE), there are five exam elements that must be achieved: Configuration, Cicode, Architecture & Redundancy, Customization & Design and Diagnostics & Troubleshooting.

Our educational methodology has proven to be effective through thousands of hours of instruction. Feedback received from customers confirms our success and drives continuous development in our services offerings. We have implemented a guided stream of learning that facilitates progression from basic through to advanced knowledge of all our products.



Custom Training: When and where you want it!

Run a training course onsite at your premises or at your chosen location, allowing your organization to train more employees while saving on travel time and expense.

Book a Training course

All courses can be booked online at www.citect.schneider-electric.com/training or contact your account manager.

Schneider Electric Industries SAS

Head Office

35, rue Joseph Monier - CS 30323

F-92506 Rueil-Malmaison Cedex

FRANCE

www.schneider-electric.com

CHV440TO122012EN

Due to evolution of standards and equipment, characteristics indicated in texts and images in this document are binding only after confirmation by our departments.

© Copyright Schneider Electric 2012. All rights reserved.

Publication & Design: Schneider Electric



OCEAN DATA SYSTEMS

The Art of Industrial Intelligence

Dream Report

User Friendly & Programming Free™
Reporting



Water and Wastewater Industrial and Municipal

Applications

40-CFR-141

EPA and State Reports

Performance & Efficiency Calculations

Monthly Operating Report (MOR)

Discharge Monitoring Report (DMR)

Electronic (eDMR)

European Environmental Agency (EEA)

EPA National Pollutant Discharge Elimination System (NPDES)

Surface Water Treatment

Safe Drinking Water Act

CFE Turbidity Reporting

Pumpage Reports

Filter Bed Performance

Lift Station Status

Maintenance Reports

Work Order Reports

SCADA and Historian Interfaces

Reverse Osmosis

EC Water Reporting

Coagulant Monitoring

Disinfectant Monitoring

Urban Waste Water Treatment (UWWT)

Asset Management

Web Data Access

Mobile Access



Water Quality Management

Whether it's water for consumption or water discharged back into the environment, the key is to deliver that water as purely as possible and as economically as possible. And as a highly regulated market, data analysis and subsequent reporting is an extremely important part of the process.

"Dream Report is designed for the Water and Wastewater market by the Water and Wastewater market."

We listened to your needs and we've addressed them head on. Dream Report has all the tools required to monitor and deliver the compliance reports you need in Water and Wastewater applications. These include reports to address USA Environmental Protection Agency (EPA) and State regulations as well as International European Environmental Agency (EEA) for both drinking water and discharge water.

Dream Report isn't a combination of business tools augmented with connectivity and automation to get by in these applications. Dream Report is a "Purpose Built" software product by a company that understands industry, your automation technologies, and your need for 24x7x365 reliability.

Dream Report is the reporting and data analysis solution, perfectly addressing the needs of this demanding vertical.

Typical Applications:

EPA Safe Drinking Water Act (SDWA) – EPA Guidelines for States, to ensure the quality of water. Dream Report will perform the calculations and generate the reports to show compliance.

40-CFR-141 – National Primary Drinking Water Regulations – These regulations are the specific regulations and requirements to be implemented with regard to the Safe Drinking Water Act. They define coliform and turbidity sampling, as well as defining the reporting requirements of each.

State Specific Reporting – Generate Monthly Operating Reports (MOR), Discharge Monitoring Reports (DMRs) and Electronic Discharge Monitoring Reports (eDMRs) and CFE Turbidity Reports. Dream Report is a flexible reporting solution with templates provided by Ocean Data Systems and its network of System Integrators, to meet federal and state requirements.

Equipment Performance Monitoring – Dream Report delivers the statistics to calculate runtimes, on-times, off-times, duty-cycles and

to evaluate operation against other variables. Is equipment operation at expected levels for these ambient conditions? Dream Report will let you know.

Energy Accounting – Municipalities are always looking to save on their energy costs, their single greatest expense. Dream Report knows how to analyze and totalize meter data, allocate that data to various operations and aid in running those assets as efficiently as possible.

Equipment Maintenance – To be as cost effective as possible and reduce the possibility of downtime, equipment should be monitored, checked on a regular basis, and maintained based on duty cycle. Dream Report delivers the math, logic and analysis to generate maintenance reports and work orders for effective management.

The Ideal System Integrator Solution

Dream Report delivers the tools for sophisticated data analysis, formatting and presentation and it delivers the tools for value added services. Reports can be password protected and System Integrators can work with Ocean Data Systems to market their report templates. Need a State report? Working with an integrator near you will result in the exact report you need, combined with the ongoing support for changes and enhancements. Contact Ocean Data Systems for more information.

Integrate with All Existing Controls

Unlike traditional business intelligence solutions, Dream Report understands automation data. Dream Report understands the structures that sources provide, data formats, time formats, alarm and message formats, and intelligently works with them all. It can even write the results back to your control systems.

Dream Report integrates with every control system through the over 60 interfaces including those for proprietary interfaces, industry standards and business (IT) standards. Connectivity typically includes access to Real-time, Alarm and Historic Data.

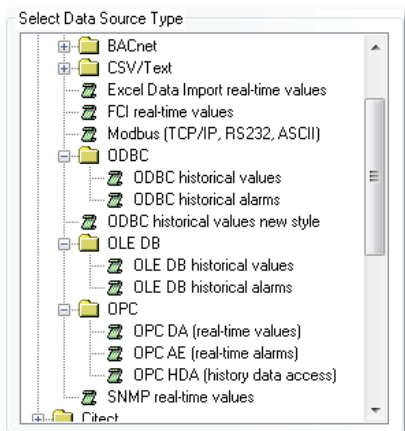
Proprietary Interfaces - Specifically built for a particular product or solution. Examples abound in Dream Report, and you can refer to our driver list for current connectivity.

Industry Standards – These include MODBUS and Open Protocols including OPC DA, OPC AE, and OPC HDA. These standards provide connectivity to any control system from Programmable Logic Controllers (PLCs) to HMI/SCADA and Distributed Control Systems

(DCS). If you have a specific connectivity need, contact Ocean Data Systems and we'll help you select an interface.

Business Standards – Includes the unique ability to automatically read and import Comma Separated Variable (CSV) and Microsoft Excel files. Dream Report also will connect to local or remote Relational Database (RDB) sources through either Open Database Connectivity (ODBC) or OLE-DB. Dream Report understands both Historic Data Logs and Alarm Message Logs.

Once data drivers are in place, Dream Report abstracts all connectivity to simple Tags, your data names, to represent that stream of information.



Open Standards Interfaces in Dream Report

Security – A Very Important Component of the Solution

Dream Report is a safe and proven solution, having been applied to thousands of applications around the world. Dream Report has been tested and approved by NIST and is listed in their database.



NVD.NIST.GOV

Security and User Authentication:

- Domain Based Security that is role oriented – The right functionality for the logged in user. Security can be node based or Windows Active Directory based.
- Report Template Version Management - Template modifications are archived and managed. Templates may be rolled back to previous versions.
- Report Signing – Reports can be electronically routed and signed. Digital signatures are applied on-line.

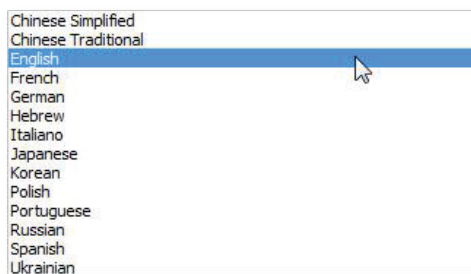
Manual Data Entry

Not all data is available programmatically. Operator Logs need to be entered and properly integrated with collected data. Manual Data Entry “Selectors” enable operators and authorized users to quickly select variables and enter corresponding results, along with timestamps to match their actual collection times. Worried about getting the data entry right? Automatic Data Validation will apply bounds to manually entered variables, ensuring that a typo doesn't make it into the record. Manual Data Entry can be human audited, validated, and corrections can be submitted. Reports can be set up to report only on validated data. Data entry can also be Mobile – entered from Smart Phones. Laboratory Information Management

Systems (LIMS) are easy to integrate with Dream Report through Manual Data Entry or the use of our Business Standard Interfaces.

Localization

Tools for your team, in the language that they dream in. Your reporting requirements aren't likely to be limited to one location. You may have facilities around the globe and your team will want to work in local languages. Dream Report supports localization, configured at the server, or defined by the user login. Standard support for over a dozen languages, switched on the fly, means Dream Report is the right solution for your diverse development team and user base.



Language Settings

Interactive Reporting

You'll want to select a template, select a facility, area, or piece of equipment and generate a report. You'll want the reports to be completely automatic, sensing process conditions to trigger their operation, but you'll also want to go back and recreate that report from last month, last year or for a particular piece of equipment. Dream Report handles all that, and the use of “Pickers” in a report gives you the interface to make date and time selections, or equipment selections. Dream Report's Web Portal delivers that capability to you in the office or away, on any device, with complete security.

Smart Reporting

Gone are the days of complicated Excel formulas for report generation. While that is always an option and Dream Report can create Excel Workbooks as its report generation, there is a more powerful solution, one that delivers the understanding of what you're trying to accomplish, and it does it simply and automatically. Dream Report “Widgets” are smart reporting objects that deliver data, analytics and visualization. You simply select the widget, drop it into your report through the WYSIWYG (What You See Is What You Get) editing environment, define its data sources and desired customizations and you are done. No hassles or macros. No errors in calculations and no scripting or software development.

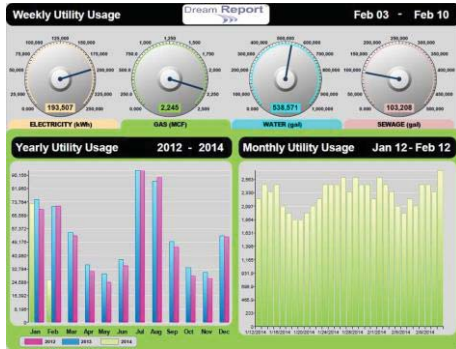
Report Design

Dream Report takes the effort and complexity out of even the most demanding reporting tasks. With connectors that understand their sources of data, to beautiful formatting and display objects, Dream Report will WOW you with its elegance. It's not just about getting data and displaying it. It's about understanding the data, using powerful analytics to turn your data into information and knowledge. Dream Report, through a wide range of Analytic Functions, delivers on that front, reducing your development efforts, improving your quality and increasing your productivity.

Widgets (Smart Objects) do most of the work for you. Need page numbers? There's a widget for that. File Name? Directory Name? Issue date, start and end times? Data displays, bar graphs, trend charts, pie charts and results tables - they are all there. Dials, gages,

tanks and more. Drag them onto the report, configure a few parameters for data source and calculation functions and you are all set. Smart Report Objects are one aspect of Dream Report's value and the analysis functions that can be attached to them are another.

The combination of purpose built calculation functions with visualization objects create the world's most sophisticated and easy to use solution for reporting and data analysis for industrial applications. Gone are the days of difficult scripting, macro development or the need for specialized IT support.



Web Portal Display with Widgets

Dream Report Delivers a Complete Array of Statistical Functions

Dream Report Analytic functions understand their purpose. They have been specially crafted to deliver the results you're expecting from the data sets your automation systems are providing.

Select Function	Caption
<input type="checkbox"/> Sum	<input type="checkbox"/> Sum
<input type="checkbox"/> Duration in the interval (hours)	<input type="checkbox"/> PeriodOfLogged
<input type="checkbox"/> Counter	<input type="checkbox"/> Cnt
<input type="checkbox"/> Logged Value Counter	<input type="checkbox"/> CntOfLogged
<input type="checkbox"/> ON Counter	<input type="checkbox"/> CntOn
<input type="checkbox"/> OFF Counter	<input type="checkbox"/> CntOff
<input type="checkbox"/> ON/OFF Counter	<input type="checkbox"/> CntOnOff
<input type="checkbox"/> Running Time	<input type="checkbox"/> RunningTime
<input type="checkbox"/> Down Time	<input type="checkbox"/> DownTime
<input type="checkbox"/> System availability	<input type="checkbox"/> Availability
<input type="checkbox"/> Standard Deviation	<input type="checkbox"/> StdDeviation
<input type="checkbox"/> Counter of alarms	<input type="checkbox"/> CntAlarm
<input type="checkbox"/> SQL Query	<input type="checkbox"/> Sql
<input type="checkbox"/> Mean Kinetic Temperature	<input type="checkbox"/> MKT
<input type="checkbox"/> Advanced Mean Kinetic Temp	<input type="checkbox"/> AdvMKT
<input type="checkbox"/> Batch ID	<input type="checkbox"/> BatchID
<input type="checkbox"/> Batch Start Time	<input type="checkbox"/> BatchStartTime

Simply Click for Function Selection

Calculation Functions

Value, Maximum, Minimum, Average, Sum, Standard Deviation, Associated Timestamps

Logged Value Counter – How many times a value is encountered

Duration Interval – Calculates time a value was in a range

Counter or Period Totals – Last variable minus first variable and rollover aware (for tracking energy meters & totalizers)

Advanced Functions

ON and OFF and Transition Counters – Delivers a count of variable transitions

Running Time – Totalizes the time a variable was on

Down Time – Totalizes the time a variable was off

System Availability – Percentage of time for a specified period during which a condition was met

Energy Management (Facility) Functions

Produced Energy – The heat energy produced by the consumption of various fuels

MONTHLY OPERATING REPORT						
FOR PUBLIC WATER SYSTEMS THAT ARE USING GROUND WATER SOURCES OR ARE PURCHASING TREATED WATER FROM ANOTHER PUBLIC WATER SYSTEM						
PUBLIC WATER SYSTEM NAME:		PWS ID No.:				
Report for the Month of: March 2014		Number of Active Service Connections this Month:				
WATER PRODUCTION						
Pumpage to storage and distribution X 1000 Gals						
Date	From Wells Directly to Distr.	From Wells to Storage Tank	Purchased Water to Distr.	Purchased Water into Storage	From SWTP or GWUDI Plant	Total Daily Production
01/02/2014	1 125.00	675.00	1 500.00	1 500.00	1 500.00	6 300.00
02/02/2014	1 350.00	825.00	75.00	75.00	75.00	2 400.00
03/02/2014	1 320.00	975.00	225.00	225.00	225.00	2 970.00
04/02/2014	300.00	75.00	750.00	750.00	750.00	2 625.00
05/02/2014	1 320.00	675.00	225.00	225.00	225.00	2 970.00
06/02/2014	150.00	30.00	1 500.00	1 500.00	1 500.00	4 680.00
07/02/2014	1 485.00	750.00	1 170.00	1 170.00	1 170.00	5 745.00
08/02/2014	1 200.00	375.00	750.00	750.00	750.00	3 885.00
09/02/2014	1 230.00	625.00	1 125.00	1 125.00	1 125.00	5 430.00
10/02/2014	1 345.00	1 200.00	900.00	900.00	900.00	5 295.00
11/02/2014	900.00	450.00	225.00	225.00	225.00	2 825.00
12/02/2014	1 200.00	675.00	375.00	375.00	375.00	3 000.00
13/02/2014	1 365.00	525.00	225.00	225.00	225.00	2 965.00
14/02/2014	600.00	225.00	225.00	225.00	225.00	1 500.00
15/02/2014	1 380.00	900.00	450.00	450.00	450.00	3 630.00
16/02/2014	750.00	375.00	150.00	150.00	150.00	1 575.00
17/02/2014	1 380.00	900.00	450.00	450.00	450.00	3 630.00
18/02/2014	1 365.00	1 200.00	900.00	900.00	900.00	5 295.00
19/02/2014	600.00	450.00	225.00	225.00	225.00	2 625.00
20/02/2014	1 200.00	675.00	375.00	375.00	375.00	3 000.00
21/02/2014	150.00	30.00	1 500.00	1 500.00	1 500.00	4 680.00
22/02/2014	1 200.00	675.00	375.00	375.00	375.00	3 000.00
23/02/2014	150.00	30.00	1 500.00	1 500.00	1 500.00	4 680.00
24/02/2014	750.00	375.00	150.00	150.00	150.00	1 575.00
25/02/2014	1 380.00	900.00	450.00	450.00	450.00	3 630.00
26/02/2014	975.00	525.00	375.00	375.00	375.00	2 825.00
27/02/2014	1 410.00	1 500.00	1 200.00	1 200.00	1 200.00	6 510.00
28/02/2014	1 425.00	1 365.00	1 170.00	1 170.00	1 170.00	6 300.00
Total	29 715.00	13 480.00	19 540.00	19 540.00	19 540.00	103 815.00
Ave	1 061.25	860.00	662.14	662.14	662.14	3 707.85
Max	1 485.00	1 500.00	1 500.00	1 500.00	1 500.00	6 510.00
Min	150.00	30.00	75.00	75.00	75.00	1 500.00

Any additional information you wish to provide:

I certify that I am familiar with the information contained in this report and that, to the best of my knowledge, the information is true, complete, and accurate.

Operator's Signature:

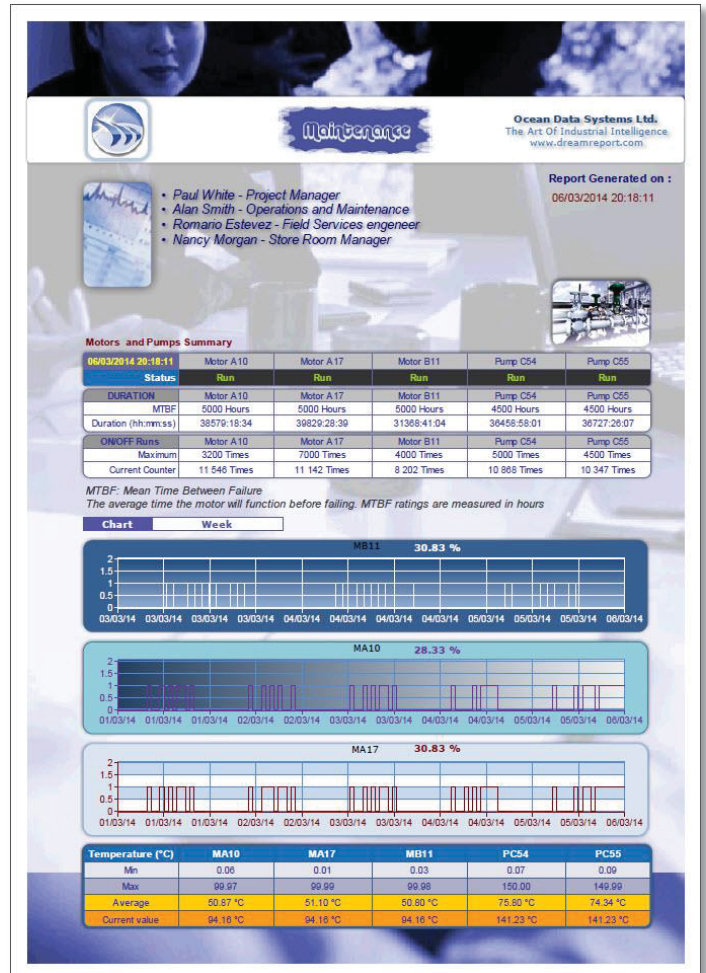
Certificate No. and Class:

Ocean Data Systems Ltd.
The Art Of Industrial Intelligence
www.dreamreport.com

Date: 17/03/2014 10:08:28

TDSG - 001 (DRAFT 1-06)

OP-PWM/OK



Produced Emissions – The emissions' byproducts from the consumption of various fuels

Alarm Analysis Functions

Alarm Counters – Calculates the number of alarms, by filter, for a specified period

SQL Functions

Direct SQL Query, with Dynamic Tokens – Use Dream Report Variables as items in a SQL Query

Pulse Analysis Functions

Excursion Analysis - Positive pulses, negative pulses, peak maximum and peak minimum functions will count variable excursions beyond a limit, over a period

Compound Data Functions

Functions over a Data Group - These functions calculate minimums, maximums, average, sum, and standard deviation of a set of other Dream Report data items

Expression Data Functions

Mathematical Expressions - Accepts a manually entered expression involving one or more statistical objects, mathematical operators and constants.

String Functions

Text String Operations - Includes concatenation, extraction, string lookups and conversions to and from numeric values

Report Storage and Distribution

Store reports in a directory. Automatically build the directory structure. Automatically name your reports. Names can include any combination of date, time, fixed text, and data variables

Distribute Reports via Email - Built-in SMTP functionality lets you distribute reports to an email list

Print Reports - Use a specific printer. Designate an automatic backup for when a printer is unavailable.

Send Reports to a Web Portal - No effort involved. Dream Report sets up IIS automatically and configures a Web Portal to display your reports (if you choose to do so), in a browser based and mobile friendly environment.

Through the benefits of HTML-5, your reports will work in any browser and on any Mobile device, iOS, Android, Windows or other. PC or MAC - it's up to you. Need a Web Dashboard of Key Performance Indicators (KPIs)? Configure a report for automatic update and you have it.



Web Portal for Interactive Report Generation

Reliability

Of crucial importance in this market. When facilities house critical operations, you must be sure the reporting is available and your systems are reliable. There is no room for error. For optimum reliability, redundancy is the solution. If reports are generated, and one printer is

unavailable, then Dream Report will automatically transfer to a backup printer. If one reporting node becomes unavailable, possibly due to a server hardware failure, a second Dream Report system will automatically recognize the failure of its counterpart and take over reporting.

A screenshot of the 'Hotbackup node configuration' dialog box. It has a title bar and a close button. The first section has a checked checkbox labeled 'This node is working in a hotbackup mode'. The second section is titled 'Set the IP address/PC name where the main node is running' and contains a text input field with 'Dream-Report-Backup-Server' and a 'Test connection' button. The third section is titled 'Checkup rate' and contains a spin box set to '5' and a label 'Seconds'.

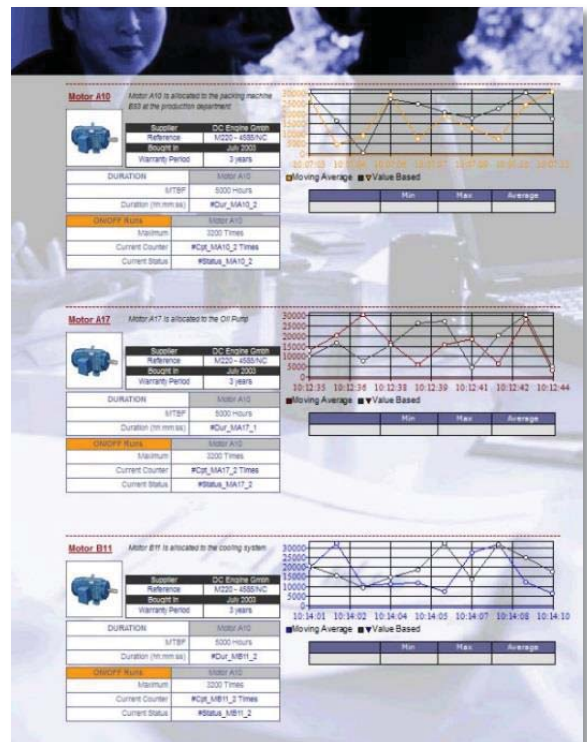
Dream Report Hot Backup Server Selection

So, What Are You Waiting For?

You may think automated report generation is just for compliance reporting, generating the necessary documentation for State or EPA compliance. That is certainly important, however, Dream Report can deliver the power of automated business intelligence to your entire organization. If you don't have an automated report generation and data analysis solution as a part of every automation system, then you could be losing out on efficiencies.

Today, when you're tasked with continuous improvement, the old adage "Out of sight, out of mind" continues to be the primary obstacle. Having business intelligence delivered to you, in a regular and automated fashion, will keep you informed of the usual, so that you can react to the unusual.

To learn more about Dream Report, visit the Endorsed Partner website at <http://software.invensys.com/>.





ENDORSED

Partner Product

Endorsed Partner

Dream Report is a product of Ocean Data Systems that is licensed, sold, delivered and supported by Schneider Electric and its subsidiaries (Invensys, Wonderware, Eurotherm, Foxboro and Indusoft).

Dream Report delivers a wide range of connectors, many specific to the Schneider Electric range of products. In addition, Dream Report delivers a host of both standards based connectors and other proprietary connectors, making Dream Report the perfect solution to integrate data from any mix of plant floor and enterprise data sources.

Dream Report is your one solution for all report generation requirements.

McAfee Endpoint Protection—Advanced Suite

Protection against zero-day attacks and help with regulatory compliance

A mobile workforce plus increased regulation could equal a security nightmare. With integrated, proactive security to combat sophisticated malware and zero-day threats, McAfee® Endpoint Protection—Advanced Suite, part of the McAfee product offering, protects endpoints when they leave your network and helps protect your network when they return. Its integrated intrusion prevention secures desktops and laptops from advanced threats. Centralized policy-based management, multiplatform support, and auditing keep all of your endpoint assets safe and compliant.

The increasing sophistication of attackers is challenging security practitioners to have the visibility and tools they need to detect and defend against advanced threats. Although every endpoint is at risk from the subtle technologies criminals use today, portable systems face extra threats. Laptops venture to hotels, coffee shops, and home offices without traditional protective layers, such as web and email gateways, network firewalls, and network intrusion prevention systems. On a Wi-Fi network, anyone might listen and pick up more than the news.

PCs can miss patches and other updates, becoming even more vulnerable to zero-day threats by simply being disconnected from the corporate network. And those patches and other updates are increasingly required for regulatory compliance. Beyond more stringent industry

regulations, your governance controls may expect you to manage distribution of sensitive data as well as appropriate web use—on-site or on the road.

McAfee® Endpoint Protection—Advanced Suite puts you in charge with broad protections, compliance controls, and unified management. Whether you want to keep viruses, hackers, spammers, data thieves, or auditors at bay, this seamless solution has the perfect combination of capabilities and cost savings.

Intelligent, Collaborative Defenses

Organizations need a strategy for threat protection, detection, and correction, as well as a security framework that empowers security components to collaborate against targeted attacks for rapid detection and action. That's why McAfee Endpoint Security 10 (included with the suite), communicates with multiple

Key Advantages

- Guard Microsoft Windows, Mac, and Linux devices against system, data, email, and web threats, and the risk of noncompliance.
- Consolidate endpoint and data security efforts with an integrated solution from one vendor—securing stronger protection at a lower cost.
- Enable increased protection immediately, with the simplicity and efficiency of centralized management and an extensible endpoint security framework.

DATA SHEET

endpoint defense technologies in real time to analyze and collaborate against new and advanced threats—blocking and quickly halting them before they impact your systems or users. Its framework helps remove duplicate technologies and connect other McAfee solutions to enable simpler management and stronger defenses. Additionally, McAfee Global Threat Intelligence (McAfee GTI) provides insights from the largest volume of observations and analysis available in the market.

Advanced Email Virus and Spam Protection

Our solution scans your inbound and outbound emails to intercept spam, inappropriate content, and harmful viruses. We can quarantine suspicious emails to prevent evolving email threats from affecting your network and users. And, a layer of antivirus on your email server prevents malware from reaching user inboxes.

Zero-Day and Vulnerability Shielding

Say goodbye to emergency patching. Exploit and intrusion prevention technologies patrol your desktops and laptops against malware, block malicious code from hijacking an application and trying to run with higher privileges, and provide automatically updated signatures that shield laptops and desktops from attack. It's safe to implement and test patches on your schedule. Combined with our patented behavioral protection, which prevents buffer overflow attacks, you get the most advanced system vulnerability coverage on the market.

Integrated Firewall

Bar unsolicited inbound traffic and control outbound traffic with our integrated firewall, which uses McAfee GTI to protect desktops and laptops from botnets, distributed denial-of-service (DDoS) attacks, advanced persistent threats, and risky web connections. Systems are also protected by allowing only outbound traffic during startup until the complete firewall policy has been enforced.

Efficient Policy Auditing and Compliance

Agent-based policy auditing scans your endpoints and documents to ensure that all policies are up to date. Organizations can measure compliance to best practice policies—ISO 27001 and CoBIT—as well as to key industry regulations.

Comprehensive Device Control

Prevent critical data from leaving your company through USB drives, Apple iPods, Bluetooth devices, recordable CDs, and DVDs. Tools help you monitor and control data transfers from all desktops and laptops—regardless of where users and confidential data go, even when users are not connected to the corporate network.

Why Choose McAfee?

- We offer a true centralized experience for administrators.
- Our integrated endpoint and security frameworks help you remove redundancies, connect other solutions, and provide an extensible architecture to build on.
- McAfee Global Threat Intelligence offers the strongest volume of threat intelligence on the market. We see and protect more than anyone else.

DATA SHEET

Proactive Web Security

Help ensure compliance and reduce risk from web surfing by warning users about malicious websites before they visit. Host-based web filtering ensures that you can authorize and block website access, protecting users and ensuring their policy compliance whenever and wherever they are web surfing. Lastly, private URLs can also be blocked, and the latest versions of multiple web browsers are supported.

Management that Lowers Operational Costs

For efficiency and comprehensive visibility across your security and compliance status, McAfee® ePolicy Orchestrator® (McAfee ePO™) software provides a single, centralized, platform that manages security, enforces protection, and lowers the cost of security operations.

Correlate threats, attacks, and events from endpoint, network, and data security, as well as compliance audits, to improve the relevance and efficiency of security efforts and compliance reports. No other vendor can claim a single integrated management platform across all these security domains. McAfee ePO software simplifies security management.

Deploy Quickly and Easily

Enable increased protection without delay. The EASI installer gets your strong protection running in as few as four clicks. Integration with McAfee ePO software lets you deploy and manage security using a single environment.

Migration Made Easy

Environments with current versions of McAfee ePO software, McAfee VirusScan® Enterprise, and the McAfee agent can leverage our automatic migration tool to migrate your existing policies to McAfee Endpoint Security 10 in about 20 minutes or less.

DATA SHEET

Feature	Why You Need It
Single integrated management	Instant visibility into security status and events and direct access to management for unified control of all your security and compliance tool with McAfee ePO software
Multiplatform	Protects the full range of endpoints required by mobile and knowledge workers, including Mac, Linux, and Microsoft Windows
Device control	Lets you monitor and restrict data copied to removable storage devices and media to keep it from leaving company control
Intrusion prevention system (IPS) and integrated firewall for desktops and laptops	Provides zero-day protection against new vulnerabilities, which reduces the urgency to patch, and controls desktop applications that can access the network to stop network-borne attacks
Anti-malware	Blocks viruses, Trojans, worms, adware, spyware, and other potentially unwanted programs that steal confidential data and sabotage user productivity
Anti-spam	Helps eliminate spam, which can lead unsuspecting users to sites that distribute malware and phish
Web control with URL filtering and safe search	Helps ensure compliance, warns users before they visit malicious websites, and protects them whether they are on or off the corporate network
Email server security	Protects your email server and intercepts malware before it reaches the user inbox
Policy auditing	Provides tightly integrated compliance reporting for HIPAA, PCI, and more

Learn More

For more information, visit www.mcafee.com/endpoint, or call us at 1 888 847 8766, 24 hours a day, seven days a week.

* The migration time is dependent on your existing policies and environment.



2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

McAfee and the McAfee logo, ePolicy Orchestrator, McAfee ePO, and VirusScan are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others. Copyright © 2017 McAfee, LLC.
417_0816
AUGUST 2016

Overcome the Attacker Advantage with McAfee Endpoint Security



SOLUTION BRIEF

Defenders Are Feeling the Pressure to Up Their Game

In digital combat, cybercriminals benefit from the success of others. Successful breaches provide the motivation and resources for further attacks, whether for financial gain, economic disruption, or corporate intelligence. Organizations of all sizes are at risk from nation-states, hacktivists, organized crime, and malicious and accidental insider threats. The knowledge and capabilities gap between attackers and defenders is mandating fundamental changes to endpoint defenses, cybersecurity's frontline.

Security practitioners are under increasing pressure to defend their organizations. To overcome the attacker advantage, endpoint defenses need to collaborate with each other and with other security technologies to quickly detect, analyze, block, and contain attacks in progress. They need to present forensic information quickly and intuitively. Moreover, they need to do all of this without adding to the complexity of the environment for IT teams or impacting the productivity and performance of the users they protect.

McAfee Endpoint Security Tilts the Battlefield in Your Favor

McAfee® Endpoint Security enables customers to respond to and manage the threat defense lifecycle and provides a collaborative, extensible framework to reduce the complexity of conventional multivendor endpoint security environments. It also provides administrators with visibility into advanced threats to speed detection

and remediation response times. Global threat intelligence and real-time local event intelligence are shared between endpoints to further aid in rapid detection and response, while management is kept simple through a true centralized console and easy-to-read dashboards and reports.

McAfee Endpoint Security is built for real-time communication between threat defenses. Events and threat insights are shared with multiple technologies to take immediate actions against suspicious applications, downloads, websites, and files. Redundancies caused by multiple point products or defenses can be found and removed, while a common endpoint architecture integrates several layers of protection to allow threat insights to be shared for faster convictions and analysis.

Integrated Advanced Threat Defenses Automate and Speed Response Times

Additional advanced threat defenses, like Dynamic Application Containment (DAC), are also available as part of the integrated McAfee Endpoint Security framework to help organizations defend against the very latest advanced threats.¹ For example, DAC will analyze and take action against greyware and other emerging malware, containing them to prevent infection.

Another available technology for advanced threat is Real Protect, which uses machine-learning behavior classification to detect zero-day malware and improve detection. The signature-less classification is performed in the cloud and maintains a small client footprint while providing near real-time detection. Actionable insights

SOLUTION BRIEF

are delivered and can be used to create indicators of attack and indicators of compromise. This can be particularly useful for lateral movement detection, patient-zero discovery, threat actor attribution, forensic investigations, and remediation. Real Protect also speeds future analysis by automatically evolving behavior classification to identify behaviors and adding rules to identify future attacks that are similar using both static and runtime features. Lastly, to immediately prevent infection and reduce the time required for IT security administrators, the client repairs the endpoint following a conviction to the last known good state.

Intelligent Endpoint Protection Lets You Know What Attackers Are Doing Now

Better intelligence leads to better results. McAfee Endpoint Security shares its observations in real time with the multiple endpoint defense technologies connected to its framework to collaborate and accelerate identification of suspicious behaviors, facilitate better coordination of defenses, and provide better protection against targeted attacks and zero-day threats. Insights like file hash, source URL, and target processes are tracked and shared not only with other defenses, but also with the client and management interfaces to help users understand attacks and provide administrators with actionable threat forensics. In addition, McAfee Threat Intelligence Exchange technology empowers adaptive defenses to collaborate with other McAfee solutions, including gateways, sandboxes, and our security information and event management (SIEM) solution. Gathering and distributing

local, community, and global security intelligence shrinks the time between attack, discovery, and containment from weeks or months to milliseconds.

Combined with McAfee Global Threat Intelligence (McAfee GTI), the McAfee Endpoint Security framework leverages the cloud to monitor and act on the full spectrum of new and emerging threats in real time across all vectors—file, web, message, and network. The existing endpoint footprint and management system is enhanced with localized and global threat intelligence to combat unknown and targeted malware instantly. Automatic actions against suspicious applications and processes quickly escalate responses against new and emerging forms of attack while informing other defenses and the global community.

Customers using DAC and Real Protect get insights into more advanced threats and the behaviors they exhibit. For example, DAC provides information on contained applications and the type of access that they attempt to gain, such as registry or memory.

For organizations interested in collecting endpoint process threat insights to hunt malware and equip incident responders, Real Protect provides insights into behaviors that have been deemed malicious and the classification of threats. These insights can be particularly helpful in uncovering how file-based malware attempts to evade detection through techniques like packing, encryption, or misusing legitimate applications.

SOLUTION BRIEF

Strong and Effective Performance Helps You Respond in Time

Intelligent defenses are of little value if they impede users with slow scans, take a long time to install, or are complicated to manage. McAfee Endpoint Security protects the productivity of users with a common service layer and our new anti-malware core engine that helps reduce the amount of resources and power required by a user's system. Endpoint scans won't impact user productivity because they only occur when the device is idle, and they resume seamlessly after a restart or shutdown. An adaptive scanning process also helps reduce CPU demands by learning which processes and sources are trusted in order to focus resources on only those that appear suspicious or that come from unknown sources. McAfee Endpoint Security possesses an integrated firewall that uses McAfee GTI to protect endpoints from botnets, distributed denial-of-service (DDoS) attacks, advanced persistent threats, and risky web connections.

Relieve the Pressure with Reduced Complexity and Increased Sustainability

The rapid growth of security products with overlapping functionality and separate management consoles has made it difficult for many to derive a clear picture of potential attacks. McAfee Endpoint Security delivers strong, long-term protection thanks to its open and extensible framework, which serves as the foundation to centralize current and future endpoint solutions management. This framework leverages the McAfee Data Exchange Layer for cross-technology collaboration with existing security investments. The integrated architecture seamlessly integrates with other products from McAfee, further reducing security gaps, technology silos, and redundancies, while improving productivity by lowering your operating costs and management complexity.

McAfee® ePolicy Orchestrator® (McAfee ePO™) software can further reduce complexity by providing a single pane of glass to monitor, deploy, and manage endpoints. Customizable views and actionable workflows in understandable language provide the tools to quickly assess security posture, locate infections, and mitigate the impact of threats by quarantining systems, stopping malicious processes, or blocking data exfiltration. It also provides a single place to manage every endpoint, other McAfee capabilities, and more than 130 third-party security solutions.

SOLUTION BRIEF

Feature	Why You Need It
Real Protect	<ul style="list-style-type: none"> ▪ Machine-learning behavior classification detects zero-day threats in near real time, enabling actionable threat intelligence. ▪ Automatically evolves behavior classification to identify behaviors and add rules to identify future attacks. ▪ Repairs the endpoint to the last known good state to immediately prevent infection and reduce administrator burdens.
Endpoint protection for targeted attacks	<ul style="list-style-type: none"> ▪ Closes the gap from encounter to containment from days to milliseconds. ▪ McAfee Threat Intelligence Exchange collects intelligence from multiple sources, enabling security components to instantly communicate with each other about emerging and multiphase advanced attacks.
Intelligent, adaptive scanning	<ul style="list-style-type: none"> ▪ Improves performance and productivity by bypassing scanning of trusted processes and prioritizing suspicious processes and applications. ▪ Adaptive behavioral scanning monitors, targets, and escalates as warranted by suspicious activity.
Advanced anti-malware protection	Protects, detects, and corrects malware fast with a new anti-malware engine that works efficiently across multiple devices and operating systems.
Proactive web security	Ensures safe browsing with web protection and filtering for endpoints.
Dynamic Application Containment	Defends against ransomware and greyware and secures “patient zero.” ²
Blocks hostile network attacks	<ul style="list-style-type: none"> ▪ Integrated firewall uses reputation scores based on McAfee GTI to protect endpoints from botnets, DDoS, advanced persistent threats, and suspicious web connections. ▪ Firewall protection allows only outbound traffic during system startup, protecting endpoints when they are not on the corporate network.
Actionable threat forensics	Administrators can quickly see where infections are, why they are occurring, and the length of exposure to understand the threat and react more quickly.
Centralized management (McAfee ePO platform) with multiple deployment choices	True centralized management offers greater visibility, simplifies operations, boosts IT productivity, unifies security, and reduces costs.
Open, extensible endpoint security framework	<ul style="list-style-type: none"> ▪ Integrated architecture allows endpoint defenses to collaborate and communicate for a stronger defense. ▪ Results in lower operational costs by eliminating redundancies and optimizing processes. ▪ Seamlessly integrates with other McAfee and third-party products to reduce protection gaps

Table 1. Key Features and Why You Need Them.

SOLUTION BRIEF

Gain the Advantage Over Cyberthreats

McAfee Endpoint Security provides what today's security practitioners need to overcome the attackers' advantages: intelligent, collaborative defenses and a framework that simplifies complex environments. With strong and effective performance and threat detection effectiveness that is proven in third-party tests, organizations can protect their users, increase productivity, and create peace of mind.

McAfee, the market leader in endpoint security, offers a full range of solutions that produce defense-in-depth by combining powerful protections with efficient management. Accelerated time to protection, improved performance, and effective management empower security teams to resolve more threats faster with fewer resources.

Migration Made Easy

Environments with current versions of McAfee ePO software, McAfee VirusScan® Enterprise, and the McAfee agent can leverage our automatic migration tool to migrate your existing policies to McAfee Endpoint Security in about 20 minutes or less.³

You'll also get these benefits from McAfee Endpoint Security:

- Zero-impact user scans for greater user productivity.
- Stronger forensic data to help you harden your policies.
- Performance improvements.
- Fewer agents to manage, along with scan avoidance, to reduce manual entry.
- Collaborative defenses that work together to defeat advanced threats.
- A next-generation framework that is ready to plug into our other advanced threat and endpoint detection

Learn More

To learn more about McAfee Endpoint Security, visit www.mcafee.com/nextgenendpoint. To learn more about how McAfee Endpoint Security complements the McAfee product portfolio, visit:

- **McAfee Endpoint Threat Protection**
- **McAfee Complete Endpoint Threat Protection**
- **McAfee Threat Intelligence Exchange**
- **McAfee Endpoint Threat Defense and Response**
- **McAfee ePolicy Orchestrator**

1. Available with McAfee Complete Endpoint Threat Protection.

2. Ibid.

3. The migration time is dependent on your existing policies and environment.



2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

McAfee and the McAfee logo, ePolicy Orchestrator, McAfee ePO, and VirusScan are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others. Copyright © 2017 McAfee, LLC. 1829_1016
OCTOBER 2016

McAfee Device Control

Prevent unauthorized use of removable storage devices

USB drives, MP3 players, CDs, DVDs, and other removable media, however useful, pose a real threat to your organization. Their small size and enormous storage capacity make it all too easy for confidential customer data and intellectual property to walk right out the front door and fall into the wrong hands—whether through loss or theft. How do you know who is storing what on which type of device? And even if the person or persons have permission to use the data, how can you be sure they are keeping it secure?

McAfee® Device Control protects critical data from leaving your company through removable media, such as USB drives, Apple iPods, Bluetooth devices, and recordable CDs and DVDs. It gives you the tools to monitor and control data transfers from all desktops and laptops—regardless of where users and confidential data go, even when they are not connected to the corporate network.

Device Control Management

Comprehensive device management helps control and block confidential data copied to removable storage devices. Device parameters, such as product ID, vendor ID, serial number, device class, and device name, can be specified and categorized. Furthermore, different policies like block or encrypt can be enforced based on the content loaded onto the devices.

Managed policies include, but are not limited to:

- Support for plug-and-play devices and removable storage devices—the removable storage device definitions can support Mac OS X-only, Microsoft Windows-only, or both
- Removable storage devices blocking or ability to make them read-only
- Content-aware protection for removable storage devices
- Integration with McAfee Endpoint Encryption for file folders and digital rights management (DRM) solutions
- File access protection for files that reside on removable storage devices.

Key Advantages

- **Unrivaled data protection:** Specify detailed hardware and content-based filtering, monitoring, and blocking of confidential data on any removable storage device.
- **Comprehensive device management:** Enable safe use of removable media devices—no need to “block all” and hinder work productivity.
- **McAfee ePO centralized management platform:** Centrally deploy and manage security policy to prevent confidential data loss via removable media.
- **Complete visibility:** Prove internal and regulatory compliance measures to auditors, board members, and other stakeholders.

DATA SHEET

- The Citrix device rule that blocks access to the thin-client device mapping: local drives, removable storage, printers, CD/DVD, clipboard, and more
- Non-system hard disks rule that blocks and monitors read-only files and provides notifications of user actions on fixed disk drives

Centralized Management Through McAfee ePO Software

Integration with McAfee® ePolicy Orchestrator® (McAfee ePO™) software offers real-time event monitoring and centralized policy and incident management. It allows for easy collection of critical-usage data, such as sender, recipient, timestamp, and data evidence. With a click of a button, McAfee ePO software offers detailed reports to prove to auditors, senior management, and other stakeholders that internal and regulatory compliance measures are in place.

Some of the advantages include:

- Deploy and update McAfee Device Control agents via McAfee ePO software.
- Manage McAfee Device Control policies and incidents via McAfee ePO software.
- Integrate with McAfee ePO software for event monitoring, centralized reporting, and auditing capabilities.
- Set role-based access control (also known as separation of duties) by McAfee ePO software for incident review.
- Notify violators and/or managers automatically.
- Access helpdesk interface.

System Requirements for McAfee ePO Server Management Console

Operating system

- Microsoft Server 2003 SP1, 2003 R2

Hardware requirements

- Disk space: 250 MB
- RAM: 512 MB, 1 GB (recommended)
- CPU: Intel Pentium II-class or higher, 450 MHz minimum

System Requirements for McAfee Device Control Endpoint

Operating systems

- Microsoft Windows XP Professional SP1 or higher
- Microsoft Windows 2000 SP4 or higher
- Mac OS X Lion, OS X Mountain Lion, and OS X Mavericks

Hardware requirements

- RAM: 512 MB, 1 GB (recommended)
- Disk space: 200 MB minimum
- Network connection: TCP/IP for remote access

Learn More

For more information, visit
www.mcafee.com/devicecontrol.

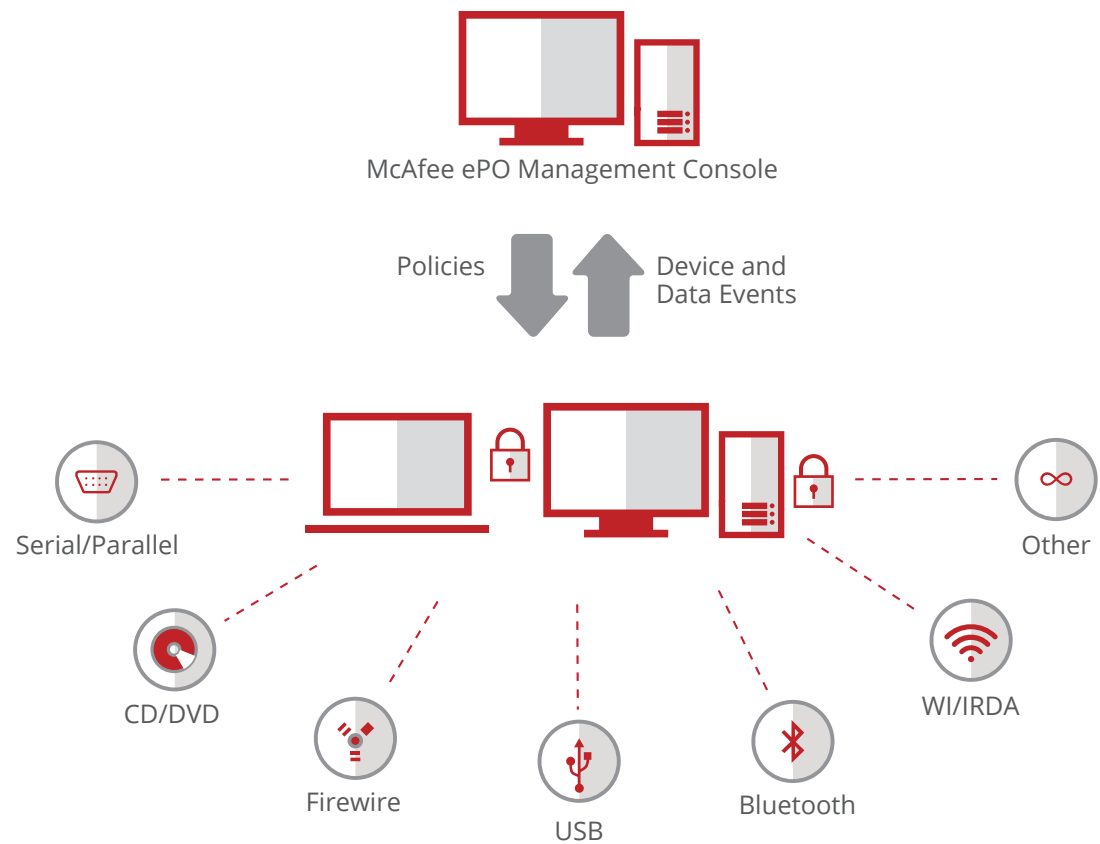


Figure 1. McAfee Device Control specifies which devices can be used and what data can be copied.



2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

McAfee and the McAfee logo, ePolicy Orchestrator, and McAfee ePO are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others. Copyright © 2017 McAfee, LLC.
61239ds_device-control_0814
AUGUST 2014

McAfee Host Intrusion Prevention for Server

Advanced vulnerability protection for servers and applications

Corporate servers store an organization's most valuable information assets and keep the business running. One of the top IT challenges is to successfully protect these servers and the applications they host from known and unknown attacks that threaten to disrupt business.

McAfee Host Intrusion Prevention for Server

McAfee® Host Intrusion Prevention for Server delivers specialized web and database server protection to maintain system uptime and business continuity, along with the industry's only dynamic and stateful firewall to shield against advanced threats and malicious traffic. In addition, it also provides signature and behavioral intrusion prevention system (IPS) protection. McAfee Host Intrusion Prevention for Server reduces patching frequency and urgency, preserves business continuity and employee productivity, protects data confidentiality, and simplifies regulatory compliance.

Defend servers and applications from attacks, and prevent data loss

Servers are increasingly the target of attacks because they house large amounts of corporate data and are also critical for performing day-to-day activities. McAfee Host Intrusion Prevention for Server secures mission-critical servers to maintain system uptime and productivity.

- Web server protection:
 - Filter HTTP requests to prevent directory traversal, Unicode, and denial-of-service (DoS) attacks.
 - Use predefined shielding policies and rules to prevent attacks and loss of data.
- Database server protection:
 - Examine database queries to prevent attacks, such as SQL injection.
 - Use predefined shielding policies and rules to ensure normal behavior and prevent tampering of data.

Advanced threat protection through our dynamic, stateful system firewall

Unlike traditional system firewalls that rely on specific rules, McAfee Host Intrusion Prevention for Server has integrated McAfee Global Threat Intelligence (McAfee GTI) network connection reputation to protect servers against advanced threats, such as botnets, distributed denial-of-service (DDoS), and emerging malicious traffic

Key Advantages

Stronger protection

- Enforce the broadest IPS and zero-day threat protection coverage across all levels: network, application, and execution.

Lower costs

- Reduce time and costs with one powerful, unified console for deployment, management, reporting, and auditing of events, policies, and agents.
- Patch endpoints less frequently and with less urgency.

Simplified compliance

- Manage compliance with easy-to-understand actionable views, workflow, event monitoring, and reporting for prompt and proper investigation and forensics.

DATA SHEET

before attacks can occur. With the increase in advanced threats, McAfee GTI offers the most sophisticated protection you can deploy.

Apply operating system and application patches less frequently, less urgently, and on your own schedule

A large percentage of exploits are released as early as three days after disclosure of the vulnerabilities. Yet, for many organizations, it may take up to 30 days to test and deploy patches for all endpoints.

McAfee Host Intrusion Prevention for Server bridges the security gap, while making the patching process easier and more efficient.

- Protection is afforded against both Microsoft and Adobe vulnerabilities. Vulnerability shielding automatically updates signatures to protect endpoints against attacks resulting from exploited vulnerabilities.
- Signature updates can be automatically and regularly downloaded for protection assurance.

Servers are no longer vulnerable during startup

Servers are vulnerable during startup because the security policies have not yet been enforced. During this vulnerable startup time, they could be subject to network-based attacks and security services could be disabled. McAfee Host Intrusion Prevention for Server

blocks attacks from occurring during this vulnerable window with firewall and IPS startup protection.

- Startup firewall protection allows only outbound traffic during startup until the complete firewall policy has been enforced.
- Startup IPS protection prevents our security services from being disabled during startup until the complete IPS policy has been enforced.

Simplified and streamlined management

Creating and maintaining multiple firewall and intrusion prevention system (IPS) policies is necessary in a large organization but is usually tedious and time-consuming. McAfee Host Intrusion Prevention for Server policy and IPS catalogs streamline that process, allowing you to create and maintain multiple firewall and IPS policies that can be applied as needed.

Optimize and simplify management further with McAfee® ePolicy Orchestrator® (McAfee ePO™) software, our single, centralized console, which helps you oversee and administer all your protection. Full integration with McAfee ePO software saves you money and time with significant operational efficiencies.

For more information, please contact a representative, or visit our website at www.mcafee.com.

System Requirements

Minimum hardware requirements

- Intel or AMD x86 and x64
- Free disk space (client): 15 MB, but 100 MB during installation
- Memory: 256 MB RAM
- Network environment: Microsoft or Novell NetWare networks. NetWare networks require TCP/IP
- NIC: Network interface card; 10 mbps or higher

Supported operating systems

- Microsoft Windows Server 2003 SP2, 2003 R2, 2003 R2 SP2 (all editions, 32- and 64-bit)
- Microsoft Windows Server 2008, 2008 SP1, 2008 SP2, 2008 R2 (all editions, 32- and 64-bit)
- SPARC Solaris 9 sun4u (32-and 64-bit)
- SPARC Solaris 10 sun4u, sun4v (32-and 64-bit)
- Red Hat Linux Enterprise 4, 32-bit
 - 2.6.9-5.EL
 - 2.6.9-5.Elhugemem
 - 2.6.9-5.ELsmp
- Red Hat Linux Enterprise 4, 64-bit
 - 2.6.9-5.EL
 - 2.6.9-5.ELsmp
- Red Hat Linux Enterprise 5, 32-bit
 - 2.6.18-8.el5
 - 2.6.18-8.el5PAE
- Red Hat Linux Enterprise 5, 64-bit
 - 2.6.18-8.el5

DATA SHEET

Compatibility with Major Virtualization Platforms

Virtualization has been adopted by practically all IT departments, and compatibility with the major virtualization platforms is essential for any product

to be successful. McAfee Host Intrusion Prevention for Server 8.0 is compatible with the three major virtualization platforms, VMware, Citrix, and Microsoft Hyper-V. The following table lists the supported products from each of these three vendors.

VMware	Citrix	Microsoft
VMware ESX–3.5 and 4.0	Citrix XenServer–5.0 and 5.5	Microsoft Hyper-V Server 2008 and 2008 R2
VMware Vsphere–4.0	Citrix Xen Desktop–3.0 and 4.0	Microsoft VDI
VMware View–3.1 and 4.0	Citrix Xen App–5.0 and 6.0	Microsoft App-V–4.5 and 4.6
VMware ThinApp–4.0 and 4.5		XP Mode on Windows 7
VMware ACE–2.5 and 2.6		
VMware Workstation 6.5 and 7.0		
VMware Player–2.5 and 3.0		

System Requirements

Supported operating systems, continued

- SUSE Linux Enterprise 10, 32-bit
 - 2.6.16.21-0.8-bigsmmp
 - 2.6.16.21-0.8-default
 - 2.6.16.21-0.8-smp
- SUSE Linux Enterprise 10, 64-bit
 - 2.6.16.21-0.8-default
 - 2.6.16.21-0.8-smp
- SUSE Linux Enterprise 11, 32-bit
 - 2.6.27.19-5-default
 - 2.6.27.19-5-pae
- SUSE Linux Enterprise 11, 64-bit
 - 2.6.27.19-5-default

Supported web servers

- Microsoft Windows
 - IIS 6.0 and 7.0
- SPARC Solaris
 - Apache 1.3.6 and later Web Server
 - Apache 2.0.42 or later Web Server
 - Apache 2.2.3 or later Web Server
 - Sun Java Web Server 6.1
 - Sun Java Web Server 7.0
- Linux (RHEL and SUSE)
 - Apache 1.3.6 or later Web Server
 - Apache 2.0.42 or later Web Server
 - Apache 2.2.3 or later Web Server

Supported database servers

- Microsoft SQL Server 2005 and 2008



2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

McAfee and the McAfee logo, ePolicy Orchestrator, and McAfee ePO are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others. Copyright © 2017 McAfee, LLC.
17802ds_hips-server_1110B
NOVEMBER 2010

McAfee Host Intrusion Prevention for Desktop

Advanced vulnerability protection for desktops and laptops

Managing security and controlling connectivity for desktop and laptop computers across an organization is increasingly challenging with the growing number of profit-driven cybercriminals and the sophisticated nature of today's threats. As workers become more mobile, that places additional pressure on IT to ensure that users connect safely to the corporate network. Additionally, organizations need zero-day protection against threats to gain more time to be able to properly prioritize, test, and deploy the necessary patches.

The Challenge

Antivirus alone is not enough, as attacks and vulnerability exploits are being released faster and are becoming more complex. The solution is to implement a proactive security strategy that prevents attacks from happening in the first place. With a proactive approach to securing endpoints, IT departments can ensure that all endpoints and confidential data are protected and business continuity is maintained.

McAfee Host Intrusion Prevention for Desktop

As an integral part of McAfee® endpoint suites, McAfee Host Intrusion Prevention for Desktop delivers unprecedented levels of protection from known and unknown zero-day threats by combining signature and behavioral intrusion prevention system (IPS) protection

with a dynamic, stateful firewall. McAfee Host Intrusion Prevention for Desktop reduces patching frequency and urgency, preserves business continuity and employee productivity, protects data confidentiality, and simplifies regulatory compliance.

Advanced threat protection through our dynamic, stateful desktop firewall

Unlike traditional system firewalls that rely on specific rules, McAfee Host Intrusion Prevention for Desktop has integrated McAfee Global Threat Intelligence (McAfee GTI) network connection reputation to secure desktops and laptops against advanced threats such as botnets, distributed denial-of-service (DDoS), and emerging malicious traffic before attacks can occur.

Key Advantages

Stronger protection

- Enforce the broadest IPS and zero-day threat protection coverage across all levels: network, application, and system execution.

Lower costs

- Reduce time and costs with one powerful, unified console for deployment, management, reporting, and auditing of events, policies, and agents.
- Patch endpoints less frequently and with less urgency.

Simplified compliance

- Manage compliance with easy-to-understand actionable views, workflow, event monitoring, and reporting for prompt and proper investigation and forensics.

With the increase in advanced threats, McAfee GTI offers one of the most sophisticated protection services you can deploy. Additional firewall features, such as application and location policies, further safeguard laptops and desktops especially when they are not on the corporate network.

Apply operating system and application patches less frequently, less urgently, and on your own schedule

A large percentage of exploits are released as early as three days after disclosure of the vulnerabilities. Yet, for many organizations, it may take up to 30 days to test and deploy patches for all endpoints. McAfee Host Intrusion Prevention for Desktop bridges the security gap, while making the patching process easier and more efficient.

- McAfee Host Intrusion Prevention for Desktop defends against zero-day exploits and unpatched vulnerabilities. Protection is provided against both Microsoft and Adobe vulnerabilities.
- Vulnerability shielding automatically updates signatures to protect endpoints against attacks resulting from exploited vulnerabilities.
- Signature updates can be automatically and regularly downloaded for protection assurance.

Endpoints are no longer vulnerable during startup

Laptops and desktops are vulnerable during startup because the security policies have not yet been enforced. During this vulnerable startup time, endpoints could be subject to network-based attacks and security services could be disabled. McAfee Host Intrusion Prevention for Desktop blocks attacks from occurring during this vulnerable window with firewall and intrusion prevention system (IPS) startup protection.

- Startup firewall protection allows only outbound traffic during startup until the complete firewall policy has been enforced.
- Startup IPS protection prevents our security services from being disabled during startup until the complete IPS policy has been enforced.

Simplified and streamlined management

Creating and maintaining multiple firewall and IPS policies is necessary in a large organization but is usually tedious and time-consuming. McAfee Host Intrusion Prevention for Desktop policy and IPS catalogs streamline that process, allowing you to create and maintain multiple firewall and IPS policies that can be applied to different groups of users and reused as needed.

System Requirements

Supported operating systems

- Windows 10
- Windows 8.1
- Windows 8
- Windows 7 SP1, 32 or 64-bit: Business, Enterprise, Ultimate
- Windows Embedded Standard 7 SP1, 32 or 64-bit
- Windows Vista 32 or 64-bit: Business, Enterprise, Ultimate
- Windows XP Professional 32-bit
- Windows XP Professional for Embedded Systems 32-bit
- Windows XP Embedded 32-bit

DATA SHEET

Optimize and simplify management further with McAfee® ePolicy Orchestrator® (McAfee ePO™) software, our single, centralized console that helps you oversee and administer all your protection. Complete integration with McAfee ePO software saves you money and time with significant operational efficiencies.

Compatibility with major virtualization platforms

Virtualization offers you lower costs, flexibility, and easier product maintenance. McAfee Host Intrusion Prevention for Desktop is compatible with many major virtualization platforms including VMware, Citrix, and Microsoft.

For more information, visit <http://www.mcafee.com/us/products/host-ips-for-desktop.aspx>.

System Requirements

Supported virtualization platforms

- Citrix XenServer: 5.0, 5.5
- Citrix XenDesktop: 3.0, 4.0, 7.5, 7.6
- Citrix XenApp: 5.0, 6.0, 6.5
- Citrix Provisioning Services 6.1
- Microsoft App-V: 4.5, 4.6
- Microsoft Hyper-V Server: 2008, 2008 R2
- Microsoft Windows Server: 2008, Hyper-V 2008, 2008 R2, 2012 R2
- Microsoft VDI (Bundle)
- MED-V: 1.0, 1.0 SP1
- SCVMM: 2008, 2008 R2
- SCCM: 2007 SP2, 2007 R2
- SCOM: 2007, 2007 R2
- VMware ACE: 2.5, 2.6
- VMware ESX: 3.5, 4.0, 5.0
- VMware ESXi 5.1
- VMware Player: 2.5, 3.0, 5.0
- VMware Server: 1.0, 2.0
- VMware Thin App: 4.0, 4.5
- VMware Vsphere 4.0
- VMware View: 4 3.1, 4.0
- VMware Workstation: 6.5, 7.0, 8.0, 9.0
- XP Mode Windows 7: 32 and 64-bit



2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

McAfee and the McAfee logo, ePolicy Orchestrator, and McAfee ePO are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others. Copyright © 2017 McAfee, LLC.
62140ds_hips-desktop_1015
OCTOBER 2015

McAfee ePolicy Orchestrator

The world's best security management software just got better

Unify the way you manage endpoints, networks, data, and compliance solutions with McAfee® ePolicy Orchestrator® (McAfee ePO™) software, the foundation of the McAfee Security Management solution. More than 30,000 customers use McAfee ePO software on more than 60 million nodes to manage security, streamline and automate compliance processes, and increase overall visibility across security management activities. With its scalable architecture, fast time to deployment, and optimization for enterprise systems, McAfee ePO software is the most advanced security management software available.

Today, more than ever, IT organizations are taking a strategic approach to security—consolidating security portfolios to reduce complexity, investing in next-generation technologies to improve protection, and integrating with existing IT assets to streamline processes. McAfee ePO software enables tens of thousands of customers to centrally manage security, achieving dramatic efficiencies.

Extensible Workflows Streamline Security and Compliance Processes

With McAfee ePO software, IT administrators can unify security management across endpoints, networks, data, and compliance solutions from McAfee and third-party solutions. McAfee ePO software provides flexible, automated management capabilities so you identify, manage, and respond to security issues and threats. You define how McAfee ePO software should

direct alerts and security responses based on the type and criticality of security events in your environment, as well as create automated workflows between your security and IT operations systems to quickly remediate outstanding issues. As a result, you save time and money—with a more effective security program. McAfee ePO software helps drive down the cost and complexity of managing security.

Comprehensive Endpoint Detection and Response (EDR)

McAfee ePO software now includes management of McAfee Active Response, delivering continuous detection of and response to advanced security threats to help security practitioners monitor security posture, improve threat detection, and expand incident response capabilities through forward-looking discovery, detailed analysis, forensic investigation, comprehensive reporting,

Connect Security to Your Business with McAfee ePO Software

Centrally manage enterprise security

- Open framework unifies security management for systems, applications, networks, data, and compliance solutions.
- Extensible platform integrates with and leverages your existing IT infrastructure.

Take action with confidence

- Get the comprehensive views and insight you need, when you need it, to proactively address security issues, both internal and external.
- Shorten time from insight to response through actionable dashboards with advanced queries and reports.
- Identify unknown assets on your network, and bring them under control with rogue system detection.

DATA SHEET

and prioritized alerts and actions. Optimized to meet the stringent endpoint detection and response (EDR) criteria, McAfee Active Response uses predefined and user-customizable collectors to search deeply across all systems to find indicators of attack (IoAs) that are not only present via running processes, but also may be lying dormant or may even have been deleted. Further, McAfee Active Response enables users to not only search for an IoA in the present, but also to alert and act in accordance with security objectives via triggers that give instructions should the IoA ever occur in the future.

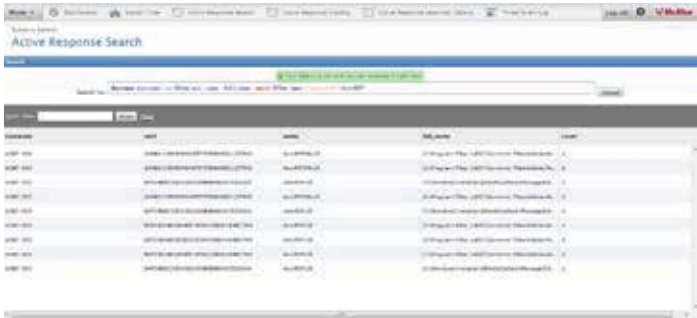


Figure 1. McAfee Active Response search user interface.

New Enhancement	Benefit
McAfee Active Response	A comprehensive endpoint detection and response feature for indicator of attack investigation and remediation
Affected systems indication	When modifying policies and tasks, administrators can see highlighted affected systems to better understand the impacts.
Automatic product installation	An improved product installation status page gives administrators enhanced product download management.
Dynamic policy and task retention	Settings from deleted extensions can be retained to preserve “gold configuration” integrity.
Enhanced disaster recovery	Recover your McAfee ePO software server and settings quickly and efficiently.
Native 64-bit support with reporting orientation	Improved performance
Policy comparison, common task orientation	Improved usability and navigation
Single page deployment	Simplified workflow and ease of implementation
URL installation of endpoint products	Easy remote endpoint installation
HTML5 UI support	Now supports the latest browsers, including IE8+, Firefox, and Safari

Table 1. New Enhancements and Benefits

Reduce complexity and streamline processes

- Guided configuration, automated work stream, and predefined dashboards make getting started a snap.
- Tag-based policy assignment precisely targets assignment of predefined security profiles to systems based on their business role or at-risk status.
- Task catalog and automated management capabilities streamline administrative processes and reduce overhead.
- A single web interface aligns security processes for maximum visibility, while a single agent reduces the risk of endpoint conflicts.

Scale for enterprise deployments

- Enterprise-class architecture supports hundreds of thousands of devices on a single server.
- Supports complex and heterogeneous IT environments
- Enterprise reporting across on-premises and Security-as-a-Service (SaaS) security information



2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

McAfee and the McAfee logo, ePolicy Orchestrator, and McAfee ePO are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others. Copyright © 2017 McAfee, .
62211ds_epo_0416
APRIL 2014

Maximize Your Automation and Process Investment

Advantages

- Secure access to the control system
- Prevent unauthorized or unwanted changes that could impact your production
- Satisfy regulatory compliance with complete audit trail of changes made to the system
- Access reports highlighting detailed changes made to program files for Rockwell Automation devices
- Maintain complete version control for all system files
- Minimize system downtime due to failed device by leveraging disaster recovery capability
- Confirm the correct and validated program is currently loaded in a device
- Scan network and discover devices (firmware) and software packages running in your plant
- Web client to visualize status of the schedule runs and logs from any mobile
- Extend coverage by adding support for 3rd party vendor devices that are not natively supported
- Reduce time to complete process

Monitoring control system changes using FactoryTalk AssetCentre, a supervisor noted the change in the audit log and found it was harmful to the process. The supervisor quickly restored an earlier copy of the control program from the AssetCentre archive, preventing any downtime.

"We saved over \$300,000 in just one incident using FactoryTalk AssetCentre to recover from potentially 2 hours of downtime".
Mining Customer



Overview

FactoryTalk® AssetCentre provides you with a centralized tool for securing, managing, versioning, tracking and reporting automation-related asset information across your entire production system. And perhaps more importantly, it can do this automatically, with limited additional management oversight or work from employees.

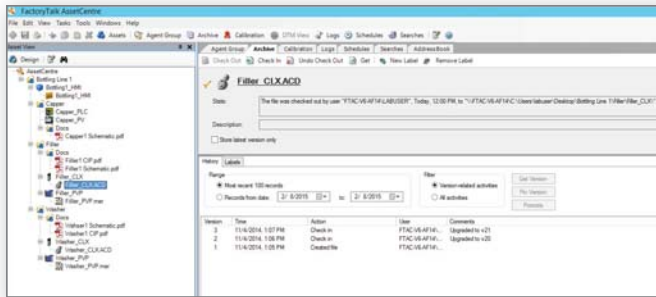
FactoryTalk AssetCentre can impact uptime, productivity, quality, employee safety and regulatory compliance. Whatever your area of concern, FactoryTalk AssetCentre and its flexible, scalable solution can help you and your organization meet your asset uptime goals.

The scalable design of FactoryTalk AssetCentre allows for easy expansion of assets and extensible (add-on) capabilities – it's adaptable from small applications to plant-wide systems. Built on a foundation that provides common base functions as well as extendable add-on capabilities, this integrated and modular design lets the system grow as your business goals and production needs change.

Base Functions

FactoryTalk AssetCentre Server provides the capability to centrally track and manage the configuration changes that occur in your facility, while providing secure access to restrict who can perform these functions. The entire breadth of the base server functionality can assist with diagnostics and troubleshooting to reduce the time needed to maintain your production assets. The base server functions include:

LISTEN.
THINK.
SOLVE.®



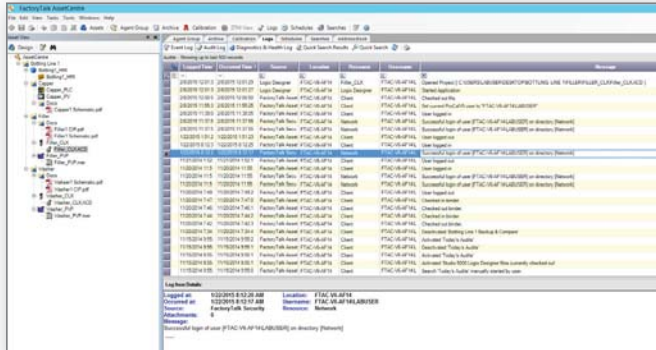
Source Control

Source control leverages the centralized database and provides automatic version control. This provides proper file management and single master relationships. Any electronic file can be put under source control – RSLogix 5000 (.acd), Microsoft files (.doc, .xls, .ppt, etc.) Computer Aided Design (CAD) files (.dwg), and others.

Audits

The Audit feature gathers information centrally that is generated by user interactions with FactoryTalk-enabled applications, including FactoryTalk AssetCentre. Audits are captured while connected or even disconnected from the network!

The audit trail consists of Logged Time, Occurred Time, Source, Location, Resource, Username and Message.



Events

The Events feature gathers system-generated information centrally from FactoryTalk-enabled applications, including FactoryTalk AssetCentre. The Event logs consist of Logged Time, Occurred Time, Source, Location, Severity and Message.

Reporting

The reporting capabilities allow scheduled or on-demand searches that include traceability information from Audit, Events or Source Control. Scheduled reports can be sent to an e-mail distribution list, or if run on demand (manually), can be printed or saved as an electronic file format of Microsoft® Excel®, Microsoft® Word, Crystal Reports®, Adobe® Acrobat®, or Rich Text Format.

Scheduler

The Scheduler is used to run periodic tasks or reports. These are assigned to FactoryTalk AssetCentre-designated computers, or agents, to leverage unused or under-utilized computing power within your facility and are load-balanced automatically across all agents in an agent group.

Total number of record found						409	
Output limited to a maximum number of records						100	
Occurred Time	Logged Time	Source	Location	Resource	Username	Attachments	Message
10/29/2014 3:0	10/29/2014 3:0	FactoryTalk As	FTAC-V6-AF14	Client	FTAC-V6-AF14	0	User logged in
3:22 PM	3:30 PM	setCentre			\LABUSER		
10/31/2014 1:2	10/31/2014 1:2	FactoryTalk As	FTAC-V6-AF14	Client	FTAC-V6-AF14	0	Design Mode
7:26 PM	7:35 PM	setCentre			\LABUSER		Selected
							Added Asset
							Parent Asset
							Path: AssetCentre New Asset
							Name: Generic Container New
							Asset Type: Generic Container
							New Asset Age
							nt Group: System Default
							Renamed Asset
							Original Asset

Security

Securing your automation system prevents unauthorized access to make changes. This is a critical first level in providing a layered security approach. FactoryTalk AssetCentre internally leverages the security provided by the FactoryTalk Services platform that can be integrated into your Windows authentication services. This standardized security model minimizes efforts to administer users and passwords on operator interfaces, historians, and engineering/ maintenance workstations. These security rights are even enforced while computers hosting FactoryTalk applications are disconnected from the network.

Tamper Detection

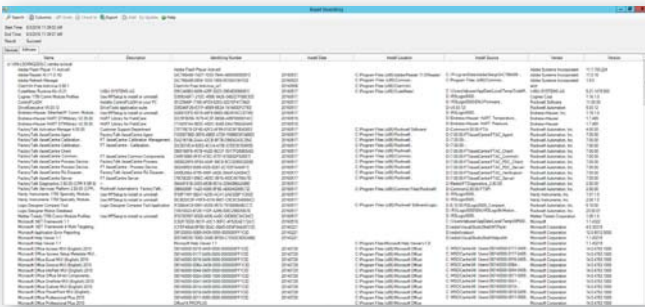
FactoryTalk AssetCentre can be configured to continuously monitor Logix controller for changes. It will detect malicious changes in real time, log activities, and create a report. For example, if a contractor walks up to a panel and connects his/her laptop to a controller directly via a usb cable, goes online and modifies the program, AssetCentre will be able to capture and report it in real time. Optionally, AssetCentre can also be configured to send this report to the stakeholders via email.

Premier Integration with Studio5000 Logix Designer

FactoryTalk AssetCentre is integrated with Studio5000 Logix Designer providing ease of use for managing versions of controller programs. Users can check-out controller programs, make edits, test out changes then check-in a new version adding appropriate comments to document the changes. This is very valuable during system commissioning or after the system is in production.

Asset Inventory Agent

Keeping track of the hundreds, if not thousands of automation assets in your facility just got easier. With the Asset Inventory Agent, you can automate discovery and track the status of all connected devices, network switches and workstation computers across an entire facility or production operation. When your search is run, it not only gives you a list of devices, but also tracks other pertinent information like software running, firmware revision, vendor name, IP address, etc. You can also manually add attributes or values to the devices and store them within the FactoryTalk AssetCentre repository to keep a complete picture of all your automation assets. As you run future scans, the compare report would list any devices added to the network or any firmware or attribute changes that occurred on the known devices.



Name	Description	Hardware	Software
1. Allen-Bradley 1756-BA01	Allen-Bradley 1756-BA01	Allen-Bradley 1756-BA01	Allen-Bradley 1756-BA01
2. Allen-Bradley 1756-BA01	Allen-Bradley 1756-BA01	Allen-Bradley 1756-BA01	Allen-Bradley 1756-BA01
3. Allen-Bradley 1756-BA01	Allen-Bradley 1756-BA01	Allen-Bradley 1756-BA01	Allen-Bradley 1756-BA01
4. Allen-Bradley 1756-BA01	Allen-Bradley 1756-BA01	Allen-Bradley 1756-BA01	Allen-Bradley 1756-BA01
5. Allen-Bradley 1756-BA01	Allen-Bradley 1756-BA01	Allen-Bradley 1756-BA01	Allen-Bradley 1756-BA01

Life cycle management – I am an engineer and working on a project to update firmware on all devices that have an end-of-life status. I don't know how many devices I have running in production. The Asset Inventory Agent will allow me to discover all of the assets with firmware revisions, IP addresses, etc. to scope my project.

Patch / Security vulnerability – I receive a note from a vendor that there is a security vulnerability identified for a specific device firmware, and they have a fix for it. Normally, I would have to manually inventory each site to figure out my risk and threat exposure. With the Asset Inventory Agent, the process is simplified greatly and I can quickly discover the affected devices and put a plan in place to mitigate the risk.

Mobile Web Client

Through this web client, you have read-only access to the Disaster Recovery Status Dashboard, Asset and Schedule Information, and Audits & Events Reports. The dashboard gives you a quick view on last search results along with drill down capability to gain more insight on failures. You can also see detailed logs and your assets under management within FactoryTalk AssetCentre.

Built on a standardized application across the Rockwell Software product family, FactoryTalk AssetCentre utilizes a

common look and feel and user experience in the mobile web client. The solution is built on HTML5 technology which allows native support for the platform of your choice spanning across iOS, Android, or Windows on a device of your choice from a smart phone or tablet, to desktop browser or a large screen TV. The client scales according to the size of the screen to present you the best possible user experience.

Disaster Recovery

FactoryTalk AssetCentre provides control system backup that is integrated with source control to provide reliable and easy access to the latest control system configuration files. The backup system can be configured to provide a comparison of the configuration file retrieved from the plant floor device with the master file stored in source control. Users can then determine if changes have been made and take appropriate action. For supported devices, a detailed report is available identifying in detail what changes were made. These operations can be performed on an ad hoc basis or configured to execute on a scheduled basis to fit your operational needs.

Disaster Recovery Assets Supported

FactoryTalk AssetCentre supports Disaster Recovery for Rockwell Automation devices and selected third-party assets natively. The FactoryTalk AssetCentre Archive can be used to manage the project files for these assets, as well as any other files that you might normally store on a computer hard drive or network share.

Disaster Recovery Assets Not Natively Supported

FactoryTalk AssetCentre can be extended to support additional 3rd party devices by using the Custom Device Plug-in capability. FactoryTalk AssetCentre can interface with the 3rd party plug-in component using command line parameters to define parameters. For example, uploading a program from a 3rd party controller and comparing it to a previous version.

Backup and Compare Schedules

Easily create Backup or Backup and Compare for any supported asset type. Schedules can be created for one or more devices, create as many schedules as you require! Set the Start time and frequency of schedule by Hourly, Daily, Weekly or Monthly. Specify by schedule and asset type backup or compare properties, i.e. Compare Options, email notifications, etc.

Notifications

The Notification feature proactively notifies designated users when predefined system events occur. E-mail notifications could include:

- Upload and compare event statuses
- Completed, aborted or failed schedules
- Rogue candidate detection

Gain Further Value with Add-on Capabilities

FactoryTalk AssetCentre has an evolving set of add-on capabilities that allow you to optimize and leverage your factory automation and process device investments. These optional capabilities expand upon the robust central features already found in the FactoryTalk AssetCentre server and allow you the ability to extend the value of the system as needs change within your manufacturing environment.

Calibration Management

The FactoryTalk AssetCentre Calibration Management capability allows for a paperless calibration solution: managing calibration requirements, specifications, schedules, calibration results and reporting. When it comes to the managing of instrument calibration and system qualifications, FactoryTalk AssetCentre offers unique advantages. Whether for a single department or an entire

organization, your workflow and oversight practices can be automated, systematized and improved – particularly in a regulated environment such as 21 CFR Part 11 Food and Drug Administration (FDA) and Good Manufacturing Practices (GMP).

Process Device Configuration

FactoryTalk AssetCentre Process Device Configuration (PDC) utilizes Field Device Tool (FDT) technology to access instrument parameters, configure and commission process devices and help with diagnostics. It gives you the ability to work with multiple vendors' instruments in one common platform, reducing overall maintenance and field time. This means you now have the freedom to choose best-in-class instruments and maintenance tools available from any of the vendors supporting FDT technology.

For more information on FDT technology, visit www.fdtgroup.org.

ADVANTAGES OF FACTORYTALK® ASSETCENTRE ADD-ON OPTIONS

FactoryTalk® AssetCentre Disaster Recovery

- Secure access to the control system
- Prevent unauthorized or unwanted changes from occurring in running processes or files
- Have a documented audit trail for Rockwell Automation devices of who made what changes and when those changes were made to device programs
- Can maintain version control for all system files
- Always know where to find the most current version of your program
- Can confirm that the correct and validated configuration or programming is currently in a device
- Extend coverage by adding support for 3rd party vendor devices that are not natively supported

FactoryTalk® AssetCentre Calibration Management

- Time to complete calibrations can be reduced by over 50%
- Allows compliance (automatic documentation and reporting)
- Helps improve staff effectiveness (ease of accessing the right information)

- Helps improve product quality and helps reduce process mishaps (instrument performing as intended)
- Helps allow a more repeatable process (not operator specific)
- Helps to lower production cost (closer to specification thresholds, removing safeties)
- Easy review of any aspect of activities
- One system!

FactoryTalk AssetCentre Process Device Configuration

- Manage installed Device Type Manager (DTM) with the DTM Catalog
- Build the DTM Networks from FactoryTalk AssetCentre client computers to the physical devices
- View and edit the configuration for a device (online or offline)
- Upload and download the configuration for a device
- Print the configuration for a device
- Manage multiple instrument types across multiple vendors
- Manage multiple instrument types across multiple protocols (HART, Profibus and Foundation Fieldbus)
- Remotely connect to instruments to diagnose and correct problems quickly

Get More Information

For ordering information, contact your local Rockwell Automation sales office or Allen-Bradley distributor. Or learn more by visiting www.rockwellsoftware.com

FactoryTalk AssetCentre, FactoryTalk Directory, FactoryTalk Security, FactoryTalk View Site Edition, Logix5000, MicroLogix, PLC-5, SLC-500, RSLinx, RSLogix 5, RSLogix 500, RSLogix 5000, PanelView Plus and Rockwell Software are trademarks or registered trademarks of Rockwell Automation, Inc. All other trademarks and registered trademarks are the property of their respective companies.

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

Americas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444

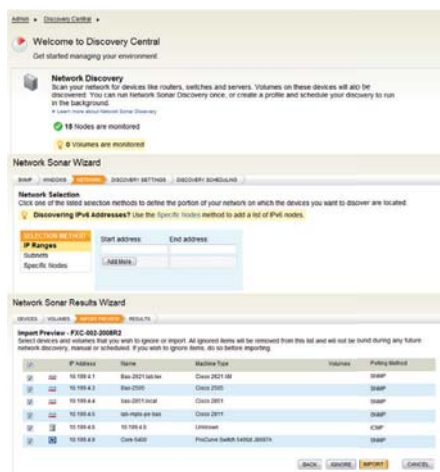
Europe/Middle East/Africa: Rockwell Automation, Vorstlaan/Boulevard du Souverain 36, 1170 Brussels, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640

Asia Pacific: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

SolarWinds is trusted by



Simplify your Network Performance Monitoring



We know the challenges you face, because we're network engineers and system administrators just like you. We know what it takes to manage complex, evolving networks. In fact, we pooled all of our "what if's" to design SolarWinds Network Performance Monitor (NPM) — a powerful, yet easy-to-use, network availability and performance management solution that delivers the critical information you need to stay on top of your evolving network.

SolarWinds NPM enables you to quickly detect, diagnose, and resolve network performance problems and outages. And SolarWinds NPM is the easiest product of its kind to deploy, use, and maintain. That means you can spend your time actually managing your network, not supporting your network management software. Plus, with one-hour, do-it-yourself deployment, you'll be monitoring immediately, instead of filling out statements of work for more consultants. See how easy network management can be with SolarWinds NPM!

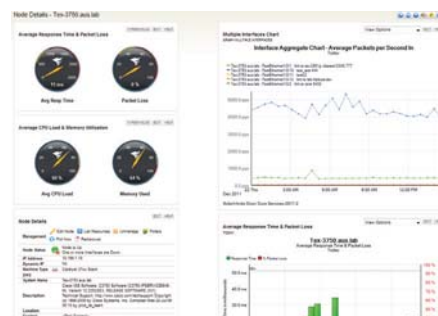
SolarWinds NPM Highlights:

- Comprehensive Network Availability & Performance Monitoring and reporting for Multi-Vendor Networks - Monitor, track the up/down status, and analyze real-time, in-depth, network performance statistics for routers, switches, wireless access points, servers, virtualized environments and any other SNMP-enabled device through an intuitive web-based user interface that provides device-by-device drill down and detailed system information.
- Automated Network Discovery & Mapping - Automatically scan your network for changes and begin monitoring new devices immediately. Display your network pictorially and visually track device status.
- Intelligent Network Alerting - Receive alerts on real issues using sophisticated alert conditions such as correlated events and sustained conditions.
- Flexible Service Status Management - Dynamically group your network resources to model your critical services and start managing end to end services in addition to your network infrastructure.

SolarWinds NPM Features

Network Availability & Performance Monitoring

SolarWinds NPM is a comprehensive performance monitoring, fault management, and network availability tool to help ensure that your network is always running at peak performance. Via a cutting-edge, customizable web interface, SolarWinds NPM gives you a unified view into the performance of thousands of



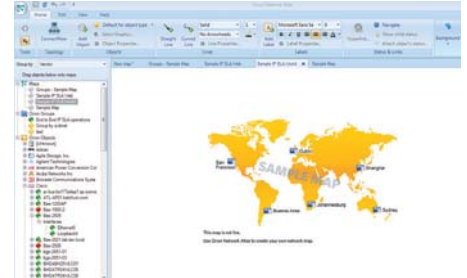
nodes and interfaces on your network. From a single web page, you can drill into any element on your network to see exactly what's happening in real time.

SolarWinds NPM's web interface provides real-time views of network performance and availability statistics, as well as detailed monitoring and analysis of data from routers, switches, servers, and any other SNMP-enabled devices. This performance monitoring data alerts you to poor network conditions like slow traffic, loss of packets, or impaired devices.

With SolarWinds NPM, you can also automatically monitor and set alerts on disk space, CPU load, and memory utilization for your network devices. With out-of-the-box support for many vendors and operating systems, SolarWinds NPM ensures that you can easily collect and alert on conditions that could potentially cause a network outage or performance degradation.

Automated Network Device Discovery

When you first deploy SolarWinds NPM, you can automatically discover all SNMP-enabled devices on your network with our Network Sonar wizard and then begin monitoring immediately. Regular scans can be scheduled to automatically discover new devices that are added to your network thus saving you valuable time by eliminating manual database entries.



Multi-Vendor Device Support

SolarWinds NPM was designed to provide out-of-the-box multi-vendor device support for today's complex network environments. SolarWinds NPM monitors availability and performance statistics for any routers, switches, firewall, VPN concentrator, wireless access point and more that support standard protocols.

ConnectNow Network Mapping

SolarWinds NPM's built-in Network Atlas allows you to view your network pictorially and visually track performance statistics in real time via dynamic network maps. With ConnectNow technology, you can even automatically display the connections between network devices on your maps. Choose from several built-in geographic map templates or import a logical image of your own network based on floor, building, department, or larger geographic location. Multiple network maps can also be nested to provide drill-down capabilities.

In literally seconds, you can drag and drop devices into their appropriate locations on the network map so that you can view the health of all network devices at a specific location; then simply click the ConnectNow button to automatically discover and display the connections between your devices. Plus, Network Atlas enables you to create your network map locally on your desktop and then export the map to SolarWinds NPM where it is immediately updated with the current status of the added nodes.

SolarWinds NPM can also display specific network maps (and specific types of network information indicated on those maps) based on the viewer's authorization level or responsibility for particular regions of the network. For example, if a device fails within a particular subnet that a user is not authorized to access, then that user's map view will not go into alert condition, as the device is outside their scope of authorization.

LUCID Web Interface

SolarWinds NPM simplifies network troubleshooting with a Web interface that is LUCID (Logical, Useable, Customizable, Interactive, & Drill-down) allowing you to manage by exception and focus on highlighted issues that cross predefined thresholds as well as customizing and viewing data in graphs, tables, maps, and top 10 lists.

Based on feedback from thousands of engineers just like you, we have identified and implemented five critical interface attributes that simplify network troubleshooting.

- Logical – The SolarWinds LUCID interface presents network performance information in a logical and intuitive manner to help you quickly make informed decisions about your network. The interface precisely presents the information you need to quickly determine if your network is suffering from poor performance.

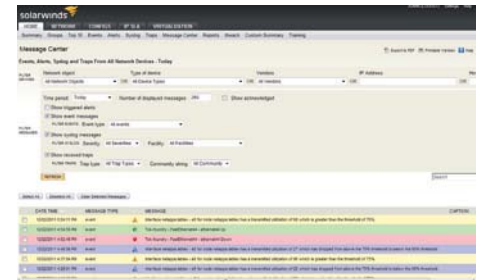
"I have continued to watch this product evolve since version 7.0 and have always found the interface and built in tools helpful and well thought out. The drill downs into more detailed reports on interfaces, nodes and resources have made this product a mainstay in the network... Definitely the best NPM product I have ever worked with."

- eusbreeves posted on solarwinds.com

- Useable – SolarWinds NPM provides a tremendous breadth of information in every view, yet the interface is very useable. Administrator tasks have all been designed to allow you to maintain SolarWinds NPM with just a few clicks of your mouse.
- Customizable – Rearrange Web resources, Top 10 views, modify time periods, and customize resources to meet your specific network environment. Easily tailor SolarWinds NPM's maps to match so you can quickly discover any performance related issues.
- Interactive – SolarWinds NPM automatically updates your network's latest performance indicators to help you quickly determine if any network issues could potentially impact users.
- Drill-down – View detailed information on virtually every device, performance indicator, and status link by simply drilling into respective hot performance indicators.

Centralized Message Center

The SolarWinds NPM Message Center is your central view for all of the notification messages about your network's performance. This consolidated view allows you to quickly troubleshoot network performance issues by analyzing SNMP trap and Syslog data from a single interface, instead of by polling various machines. Events and alerts are also routed to this interface, allowing you to perform manual event correlation and basic root cause analysis.



Intelligent Network Alerting

SolarWinds NPM enables you to quickly and easily configure powerful network alert engines to respond to hundreds of different network scenarios, including multiple condition checks. These network alerts help you recognize and correct issues before your users experience performance degradation or availability issues. With alerting support for correlated events and sustained conditions, SolarWinds NPM ensures that you don't get paged at 3am unless there is a critical issue.

Additionally, SolarWinds NPM can automatically escalate network alerts until a problem is resolved.

SolarWinds NPM includes more than sixteen built-in network alert delivery methods and responses, including email, pages, SNMP traps, text-to-speech, syslog messages, and the launching of an external application.

Dynamic Service Groups

Simplify monitoring for large and complex IT environments by grouping network devices, interfaces, servers, or volumes by virtually any category. With dynamic service groups, you can monitor and aggregate views of servers, routers, switches, interfaces, and application groups by service such as email, location, department or manufacturer.

Customizable Performance & Availability Reports

SolarWinds NPM's advanced reporting engine enables you to quickly generate custom network reports that can be printed or viewed on the web. Shipping with hundreds of built-in reports, SolarWinds NPM makes it easy to report on performance data over specific time periods or by network segment.

If you can't find a network report that matches your criteria, check out [thwack](#), SolarWinds online community, where customers have generated hundreds of reports that you can easily import into SolarWinds NPM. Plus, you can quickly customize built-in network reports and community-generated templates using SolarWinds NPM's web interface, or you can even create completely customized reports using SQL commands. SolarWinds NPM's reports can be modified to limit the information contained in the report by user profile, enabling you to generate reports for specific departments or recipients.

Integrated Wireless Polling

SolarWinds NPM's Integrated Wireless Poller enables you to easily manage wireless thin and autonomous access points and their associated clients. Now SolarWinds NPM can monitor your wireless devices alongside your wired devices and provide you with alerts, reports, and Top 10 lists for your wireless infrastructure!

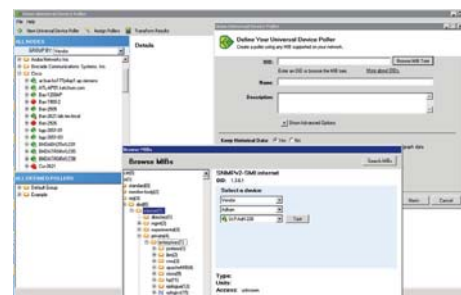
Custom MIB Poller

Out of the box, SolarWinds NPM ships with MIB support that includes a MIB database that covers the vast majority of common network devices. But for that handful of odd devices that are in your network – or for newer devices that have MIB tables – you can now collect valuable and highly detailed management data.

SolarWinds NPM makes it easy to create a custom poller to monitor any SNMP-enabled device value that has a MIB, including virtually any statistic that a network device records. Examples include monitoring temperature on a switch, fan speed on a router, and battery status on a UPS. In addition to creating custom MIB pollers, SolarWinds has an extensive database of MIB information to determine the English name for each OID and the MIB to which it belongs.

You can also customize how you want the collected data displayed for graphing, alerting, and reporting purposes. And, using the MIB Transformation Wizard, you can convert MIB values into the units of measurement that are most useful to you. Choose from a list of common transformations, such as converting monitored CPU temperatures from Celsius to Fahrenheit, or create your own multi-MIB formulas to display, for example, the average interface throughput on a router.

Additionally, you can collect detailed information stored in device MIB tables and easily create formulas such as the min, max, average, or sum of MIB entries in the same column. You can even export MIB pollers or transformations you've created, or import those created by others.



Microsoft Active Directory™ Integration

Leverage your existing Microsoft Active Directory user accounts to allow users to log into SolarWinds NPM. Users and groups can automatically login using custom username/password or optionally use an AD pass-through login to bypass the login screens altogether.

As an administrator, you can customize each account and specify which types of information are displayed within the SolarWinds NPM interface for a particular department, group, or user. This ensures that only the people who need to view specific information have access to it, providing an increased level of internal security.

VSAN Monitoring and Reporting

With dedicated views into VSAN devices, you'll be able to quickly see how much traffic is passing through each device and interface, which ports belong to which VSANs, which type of media each device is leveraging, and much more. Threshold-based alerting allows you to get ahead of any VSAN performance issues so you're the first to find (and fix) any issues.

Cisco Unified Computing System Support

By uniting computing, networking, storage access, and virtualization into a next - generation data center platform, Cisco's Unified Computing System (UCS) revolutionizes the virtualized environment. SolarWinds NPM simplifies the management of your Cisco Unified Computing System components by providing a unified view of data center network health through a single pane of glass.

Mobile Views

With SolarWinds NPM's mobile views, you can monitor network performance from popular mobile Web browsers including iPhone®, Blackberry®, and Android.

Do-It-Yourself Deployment

Deploying SolarWinds NPM is a simple three-step process. First, install and configure SolarWinds NPM using a simple wizard interface. Next, let SolarWinds NPM automatically discover your network. Finally, begin monitoring your network for fault and performance issues. You'll be done in less than an hour.

Even better, with SolarWinds NPM's intuitive web interface, you won't need to attend training classes, read books with large animals on the cover, or pour through manuals to start being productive with NPM from day one.

SolarWinds NPM Complementary Solutions

SolarWinds complementary solutions provide integration points with SolarWinds NPM allowing you to extend the capabilities of SolarWinds NPM to network traffic analysis, network change and configuration management, IP address management, user tracking, VoIP infrastructure & WAN performance monitoring, server & application monitoring, and end-user experience monitoring all in a customizable, fully integrated web console.

- NetFlow Traffic Analyzer
- Network Configuration Manager
- IP Address Manager
- User Device Tracker
- IP SLA Manager
- Server & Application Monitor
- Synthetic End User Monitor

SYSTEM REQUIREMENTS	
CPU Speed:	3.0 GHz
Hard Drive Space	20 GB
Memory	3 GB
Operating System	Windows 2003 and 2008 Server (32-bit or 64-bit) including R2, with IIS installed, running in 32-bit mode; .NET 3.5 Framework
Database	SQL Server 2005 SP1/ 2008 (Express, Standard, or Enterprise)

MODEL	MANAGES:
SL100	Up to 100 elements
SL250	Up to 250 elements
SL500	Up to 500 elements
SL2000	Up to 2000 elements
SLX	Unlimited elements

"The web-based interface provides instant, constant updates as to the status of our network to helpdesk staff, tech staff and management."

- pob posted on solarwinds.com



Backup Exec™ 16

Powerful, flexible, and trusted data protection designed for virtual, physical and cloud environments

Overview

Backup Exec™ 16 delivers powerful, flexible, and trusted data protection designed for your entire infrastructure regardless of platform: virtual, physical or cloud. With Backup Exec, you get fast, reliable protection of data and systems at every level, as well as advanced integration with the most recent releases of Microsoft® Server, Microsoft® Hyper-V and VMware® vSphere®. In a matter of minutes, you can recover anything including VMs, servers, databases, files, and granular application objects. Protect one to thousands of virtual machines from a single user console, optimizing performance and efficiency. Backup Exec saves time, money and helps ensure your critical information is always protected and easily recoverable.

Powerful

When you can solve more problems with less complexity, you have a simple yet powerful solution to improve administrative productivity. Backup Exec can help you meet business expectations for backup and recovery, reduce storage costs, secure confidential data, achieve regulatory requirements, and eliminate niche backup tools from your infrastructure.

- **Fast and reliable backup and recovery**—Backup Exec enables you to meet your organization's data protection expectations by reducing the time it takes to back up and recover critical information, apps and servers. With Backup Exec you can mitigate the risk and cost of downtime by using a wide variety of flexible backup and recovery methods. Whether you are using disk, tape, or cloud, your information can be easily and reliably recovered.
- **Advanced integration with VMware and Hyper-V**—Backup Exec offers full protection for your virtual environment and Software-Defined Data Center including new Software-Defined Storage features like VMware® Virtual SAN and Virtual Volumes. Recover what you need, when and where you need it. Easily create stand-by virtual copies of your physical systems for disaster recovery in minutes, or for

general P2V migrations. Backup Exec addresses VM sprawl by automatically identifying and protecting new VMs as they appear so you can be assured your VMs are protected from day one.

- **Save more, store less**—Flexible global de-duplication in Backup Exec helps you solve for growing data challenges, regardless of how much your data changes. It helps minimize backup windows, decrease network traffic, and reduce disk space required for storing backup data. Backup Exec de-duplicates across all virtual and physical backup jobs, reducing storage costs over other, individual job-based methods.

Key Features and Benefits

- Single solution for virtual, physical and cloud environments simplifies backup and eliminates the cost and complexity of multiple point products.
- Fast virtual machine snapshots through deep integration with Microsoft® Volume Shadow Copy Service (VSS) and VMware vStorage™ APIs for Data Protection (VADP) minimizes CPU, memory, and I/O load performance impacts on the virtual host.
- Instant Recovery of VMware and Hyper-V virtual machines provides an immediately usable copy of the server and data for DR, compliance, testing and application deployment.
- Integrated global deduplication and change block tracking allows you to protect more data while minimizing disk space required for backup files.
- Veritas-certified compatibility with virtually any storage device including disk, tape and cloud

means Backup Exec supports your organization's storage strategy, not the other way around.

- Integrated bare-metal, physical to virtual (P2V) and virtual to physical (V2P) recovery helps minimize downtime and disruption.

Flexible

Not every backup solution has the flexibility to protect all of your organization's information – whether virtual, physical or cloud. Choose the data protection architecture that works for you, rather than letting the software dictate your setup. Backup anything to virtually any storage device, and restore nearly anywhere. From VMs, to entire servers, applications, single files and folders or granular application objects, Backup Exec is the single solution for all of your data protection needs.

- **Virtual and physical data protection in a single solution**

—Lowering costs and simplifying backup tasks starts with deploying a single solution that is designed for your entire infrastructure regardless of platform: virtual, physical, or cloud. Deeply integrated with VMware, Microsoft and Linux platforms, Backup Exec can protect one to thousands of servers and virtual machines all from the same user console, providing optimal performance and efficiency. Scalability is an important consideration in backup and recovery, and Backup Exec supports you as your organization grows.

- **Hybrid architectures to disk, tape, and cloud**—Backup Exec provides the flexibility to protect VMware and Hyper-V environments using agents or agentless methods, in addition to Microsoft and Linux-based physical machines, whether local or remote. Flexible target options allow you to write to virtually any storage device including disk, tape, hosted storage, or directly to public cloud services such as Amazon S3, Google Cloud Storage and Microsoft Azure. Gateway devices such as Amazon Storage Gateway or Microsoft StorSimple permit rapid migration to economical cloud storage.

- **Fast, efficient, and versatile recovery**

—Backup Exec recovers data rapidly at any level of granularity, “from anywhere, to anywhere” with a single pass backup. In a few simple clicks, you can recover data from virtual machines and physical servers, including entire applications, individual objects, files, folders, and granular application items from Microsoft® Exchange, Active Directory®, SQL Server®, and SharePoint®. Backup Exec intelligently indexes and catalogs backup data so you don't waste valuable time and disk

space mounting backup jobs, determining what's inside, and searching for specific data. Backup Exec efficiently restores data directly from the backup, which simplifies and speeds up recovery when you need it most. Backup Exec also provides built-in disaster recovery (DR) for physical and virtual systems to help minimize downtime, mitigate risk and eliminate business disruption. In the event of a disaster, Backup Exec can recover an entire server from a bare metal state to the same or dissimilar hardware in minutes, not hours or days. It can also convert your physical servers or their backups into virtual machines. Protected virtual machines can be rapidly spun up from the backup set for immediate use.

Trusted

Complex backup and recovery products can be inefficient, time consuming, and expensive to manage. Through intuitive wizards and insightful dashboards, Backup Exec is easy to implement, use and manage, whether you are upgrading from a previous version or switching from a competitive product.

- **Easy to manage**—Quickly track and monitor every backup and recovery job through an easy-to-use interface with intuitive dashboards and wizards. In a few simple clicks, you can set backup jobs, view backup status, and perform quick recoveries. Rather than using complex policies, save time and simplify the implementation of backup protection with a visual workflow that lets you replicate data on-premise, off-site or to the cloud. In addition, the centralized administration console in Backup Exec delivers scalable management of distributed sites and helps reduce the time and resources needed to manage your backup operations.
- **Superior visibility**—Backup Exec gives you visibility into your entire backup and recovery infrastructure so that you can take action when needed. Easily perform a granular search of backed up data including mailbox data by subject, Microsoft SQL databases by name, or SharePoint data by document name. Configure Backup Exec to intelligently browse your environment and discover servers, VMs and other data at risk.
- **Flexible licensing**—Backup Exec 16 is a cost-effective solution that's easy to acquire, license, and deploy. Flexible licensing options for on-premise software include per TB, per socket or per module (agents and options). With Backup Exec you benefit from the ability to choose the right licensing model for your environment—all at affordable prices.

Support Services

No matter the size of your organization, a service interruption can result in significant losses. Fortunately, the Veritas technical support team is here to help. Veritas

Essential Technical Support is included with your Backup Exec purchase and provides 24 x 7 expert problem resolution. In addition, while your support contract is active, you can upgrade your appropriate Backup Exec licenses to newer versions as they become available — at no additional cost.

System Requirements

For a complete list of system requirements and supported devices, please refer to the Backup Exec 16 hardware and software compatibility list: backupexec.com/compatibility

Available Editions, Agents, and Options

Backup Exec Editions

Backup Exec is available as on-premise software with three licensing options—per TB, per socket, per module.

- Backup Exec 16 Capacity Edition Lite (per front-end TB)
- Backup Exec 16 Capacity Edition (per front-end TB)
- Backup Exec 16 V-Ray Edition (per occupied socket)
- Backup Exec 16 (a la carte: per module, media server, agent or option)

Backup Exec Agents and Options

Backup Exec provides scalable, easy-to-manage backup and recovery for virtual and physical environments. Backup Exec Agents and Options expand the features and functionality of Backup Exec to support critical applications, databases, storage configurations and much more.

- Backup Exec Capacity Edition Lite includes a Backup Exec Server, Agent for VMware and Hyper-V, Agent for Windows, Agent for Applications and Databases, and Agent for Linux
- Backup Exec Capacity Edition includes all Backup Exec Agents and Options
- Backup Exec V-Ray Edition includes Agent for Applications and Databases, Agent for VMware and Hyper-V and Deduplication Option (additional Agents and Options can be added and licensed as required)
- Backup Exec a la carte: Agents and Options are licensed individually

Agents

- Agent for Applications and Databases
- Agent for VMware and Hyper-V
- Agent for Windows®
- Agent for Linux
- Remote Media Agent for Linux

Options

- Agent for Applications and Databases
- Deduplication Option
- Enterprise Server Option
- Library Expansion Option
- NDMP Option
- Virtual Tape Library Unlimited Drive Option

Testimonials

"So how would ESG Lab rate Backup Exec in terms of virtual machine backup best practices? Our testing indicates that Backup Exec has hit every best practice in the center of the target Bullseye."

-Vinny Choinski, Senior Lab Analyst and Kerry Dolan, Lab Analyst, ESG

"I've used other backup solutions in a virtualized environment with varying degrees of success. But for me, the ability to back up a virtual machine image as well as the files inside it—or restore an entire virtualized application or the granular data in it, whether it's Exchange, SharePoint or SQL—that's what makes Backup Exec far more compelling than its competitors."

-Paul Flatt, Infrastructure & Support Manager Mitre 10 (NZ) Limited

"Our backups complete with near 100% reliability and restores are consistently successful with zero fuss. It just works."

-Brandon Mosak, IT Director Task Force Tips Inc.

"Nothing else on the market comes close for performance and usability."

-Terry Green, IT Manager AutoChair

More Information

Visit our website

<https://www.veritas.com>

To speak with a Product Specialist in the U.S.

Call toll-free 1 (866) 837 4827

To speak with a Product Specialist outside the U.S.

For specific country offices and contact numbers, please visit our website.

About Veritas Technologies LLC

Veritas Technologies LLC enables organizations to harness the power of their information, with solutions designed to serve the world's largest and most complex heterogeneous environments. Veritas works with 86 percent of Fortune 500 companies today, improving data availability and revealing insights to drive competitive advantage.

Veritas World Headquarters

Veritas Technologies LLC
500 East Middlefield Road
Mountain View, CA 94043 USA
+1 (650) 527 8000 | 1 (866) 837 4827 | www.veritas.com

ATTACHMENT 1 – CATALOGUE AND DATASHEET

ACCESSORIES

Rittal – The System.

Faster – better – everywhere.

TopTherm fan-and-filter units with EC technology – SK 3245.500

Date : Feb 8, 2018

ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

IT INFRASTRUCTURE

SOFTWARE & SERVICES

FRIEDHELM LOH GROUP



TopTherm fan-and-filter units with EC technology – SK 3245.500

created: 08.02.2018 build on www.rittal.com/il-en



Product description

Description: Energy-efficient version of the TopTherm fan-and-filter units with diagonal fan technology. Fans 3240.500 to 3245.510 may be controlled and monitored. The fan may be activated via the control interface with tacho signal output integrated as standard, and monitoring of the fan speed and function is supported.

Colour: RAL 7035

Protection category IP to IEC 60 529: IP 51
with standard filter and hose-proof hood: IP 56
with standard filter and additional fine filter mat: IP 52

Protection category NEMA: with hose-proof hood: NEMA 1
with hose-proof hood: NEMA 12
with hose-proof hood: NEMA 3
with hose-proof hood: NEMA 3R

Supply includes: Complete unit ready to install, including filter mat

Note: For even more efficient operation or for monitoring the fan-and-filter units, we recommend the use of an EC speed control for EC fan-and-filter units

Product features

Air throughput (unimpeded air flow): At 50 Hz: 900 m³/h

Air throughput with outlet filter including standard filter mat (quantity x order)
1 x 3243200: 680 m³/h
2 x 3243200: 820 m³/h

number, output 50/60
Hz):

Control interface:	yes
Rated operating voltage:	200 V - 240 V, 1~, 50 Hz/60 Hz
Dimensions:	Width: 323 mm Height: 323 mm
Required mounting cut-out:	Width: 292 mm Height: 292 mm
Build depth:	25 mm
Installation depth:	130.5 mm
Temperature range:	Bearing: -25°C...+70°C Operation (environment): -25°C...+55°C
Power consumption P_{sub-el-subcl}:	At 50 Hz: 165 W
Rated current (max.):	At 50 Hz: 1.33 A
Miniature circuit-breaker/fuse:	4 A
Noise level:	At 50 Hz: 72 dB(A)
Diagonal fan:	Diagonal, EC motor
Packs of:	1 pc(s).
Weight/pack:	3.46 kg
EAN:	4028177652262
Customs tariff number:	84145915
ETIM 6.0:	EC000320
ETIM 5.0:	EC000320
eCl@ss 8.0/8.1:	27180716
eCl@ss 7.0/7.1:	27180716
eCl@ss 6.0/6.1:	27180716

**Product description
(long):**

SK fan and filter units TopTherm, 900 m³/h, 200-240 V, 1~, 50/60 Hz, WHD: 323 x 323 x 25 mm, EC-Technology

Approvals**Approvals:**

Approval overview
CSA
UL + C-UL - FTTA
UR + C-UR

Certificates:

EAC

Declarations:

Declaration of conformity

Rittal – The System.

Faster – better – everywhere.

Compact light – SZ 4140.010

Date : Feb 6, 2018

ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

IT INFRASTRUCTURE

SOFTWARE & SERVICES

FRIEDHELM LOH GROUP



Compact light – SZ 4140.010

created: 06.02.2018 build on www.rittal.com/il-en



Product description

Benefits:	<p>Slimmer: Around 50% less height and depth and therefore around 75% less volume than conventional lights</p> <p>Faster: Universal fast attachment to the TS slots via clips, screws, or powerful magnets (optional). Simply slide in at the side or rear, fit the light, and it's done!</p> <p>Door-operated switch can also be connected via a 2-pole connector</p> <p>Transparent light cover, grooved on the inside</p>
------------------	--

Colour:	Similar to RAL 7035
----------------	---------------------

Protection category IP to IEC 60 529:	IP 20
--	-------

Supply includes:	<p>Compact light with clip and screw mounting kits</p> <p>Light</p> <p>Light cover</p> <p>Connection cable</p> <p>Assembly parts</p>
-------------------------	--

Note:	Door-operated switch can also be connected via a 2-pole connector
--------------	---

Note on Model No.:	Cable deflector across rear possible
---------------------------	--------------------------------------

Product features

Dimensions:	<p>Width: 455 mm</p> <p>Height: 59 mm</p> <p>Depth: 24 mm</p>
--------------------	---

Rated operating voltage:	<p>100 V - 240 V, 1~, 50 Hz/60 Hz</p> <p>Voltage tolerance: $\pm 10\%$</p>
-------------------------------------	---

Installation options:	TS horizontal section of the roof frame: direct TS, SE vertical section: direct SE extrusions at the front and rear of the roof frame: direct SE extrusions at the side of the roof frame: direct AE, CM, TP: with magnet mounting kit AE: with rail for interior installation
Mounting dimensions:	Mounting distance – clip/magnet: 400 mm Mounting distance – screw attachment: 475 mm
Operating temperature:	Operation (environment): -15°C...+45°C Bearing: -20°C...+70°C
Rated current:	At 230 V/50 Hz: 0,045 A - 0,088 A At 110 V/60 Hz: 0,083 A - 0,149 A
Power consumption:	8 W
Equipment (electrical):	Ballast: Wide-range electronic ballast Light: Fluorescent lamp T5 Length of connection cable: 3 m Colour of cable: Yellow Switch (type): Integral, on/off/door-operated switch mode
Rated insulation voltage:	500 V DC/1s
Rated impulse withstand voltage, phase to earth:	1000 V AC
Rated impulse withstand voltage, phase to phase:	500 V AC
Protection category:	II (all-insulated)
Connection options:	Integral connection cable with open end Door-operated switch
Light – installation type:	Screw-fastening Clip attachment Magnetic attachment (accessory)
Cable deflector across rear possible:	yes
Light cover:	yes
Packs of:	1 pc(s).
Weight/pack:	0.6 kg
EAN:	4028177522725

Customs tariff number:	94054095
ETIM 6.0:	EC000321
ETIM 5.0:	EC000321
eCl@ss 8.0/8.1:	27189241
eCl@ss 7.0/7.1:	27189241
eCl@ss 6.0/6.1:	27189241
eCl@ss 5.1/5.1.4:	27189241
Product description (long):	SZ Compact light, WHD: 455x59x24 mm, 8 W, 100-240 V, 50/60 Hz, Integral on/off/door-operated switch mode, ENEC
Approvals	
Certificates:	EAC
Declarations:	Declaration of conformity



POWER SUPPLY

- AC 100-240V Wide-range Input
- Width only 65mm
- Efficiency up to 94.0%
- ATEX and IECEx Approved
- -C1 Version with Conformal Coated PC-Board
- Excellent Partial Load Efficiency
- 20% Output Power Reserves
- Safe Hiccup^{PLUS} Overload Mode
- Easy Fuse Breaking due to High Overload Current
- Active Power Factor Correction (PFC)
- Minimal Inrush Current Surge
- Full Power Between -25°C and +60°C
- DC-OK Relay Contact
- Current Sharing Feature for Parallel Use
- 3 Year Warranty

GENERAL DESCRIPTION

The Dimension C-Series are cost optimized power supplies without compromising quality, reliability and performance. The C-Series is part of the DIMENSION power supply family. The most outstanding features of CPS20.241 are the high efficiency, electronic inrush current limitation, active PFC, wide operational temperature range. The small size is achieved by a synchronous rectification and further technological design details.

The C-Series includes all the essential basic functions. The devices have a power reserve of 20% included, which may even be used continuously at temperatures up to +45°C. Additionally, the CPS20.241 can deliver about 4 times the nominal output current for 15ms which helps to trip fuses on faulty output branches.

High immunity to transients and power surges as well as low electromagnetic emission, a DC-OK relay contact and a large international approval package for a variety of applications makes this unit suitable for nearly every situation.

SHORT-FORM DATA

Output voltage	DC 24V	
Adjustment range	24 - 28V	
Output current	20A	at 24V, amb <60°C
	24A	at 24V, amb <45°C
	17.1A	at 28V, amb <60°C
	20.6A	at 28V, amb <45°C
Output power	480W	ambient <60°C
	576W	ambient <45°C
Output ripple	< 50mVpp	20Hz to 20MHz
AC Input voltage	AC 100-240V	-15%/+10%
Mains frequency	50-60Hz	±6%
AC Input current	4.36 / 2.33A	at 120 / 230Vac
Power factor	0.99 / 0.95	at 120 / 230Vac
AC Inrush current	typ. 9 / 7A peak	at 120 / 230Vac
Efficiency	92.7 / 94.0%	at 120 / 230Vac
Losses	37.8 / 30.6W	at 120 / 230Vac
Temperature range	-25°C to +70°C	operational
	Derating *)	+60 to +70°C
Hold-up time	typ. 26 / 26ms	at 120 / 230Vac
Dimensions	65x124x127mm	WxHxD
Weight	1000g / 2.2lb	

*) between 100-85Vac see chapter 15

ORDER NUMBERS

Power Supply	CPS20.241	24-28V Standard unit
	CPS20.241-C1	Conformal coated unit
Accessory	ZM2.WALL	Wall mount bracket
	ZM13.SIDE	Side mount bracket
	YR40.242	Redundancy module
	YR40.245	Redundancy module

MARKINGS



INDEX

	Page		Page
1. Intended Use	3	20. Physical Dimensions and Weight	18
2. Installation Requirements	3	21. Accessories	19
3. AC-Input	4	21.1. ZM2.WALL - Wall Mounting Bracket	19
4. DC-Input	5	21.2. ZM13.SIDE - Side Mounting Bracket	19
5. Input Inrush Current	5	21.3. Redundancy Modules	20
6. Output	6	22. Application Notes	21
7. Hold-up Time	8	22.1. Peak Current Capability	21
8. DC-OK Relay Contact	8	22.2. Back-feeding Loads	22
9. Efficiency and Power Losses	9	22.3. External Input Protection	22
10. Lifetime Expectancy and MTBF	10	22.4. Output Circuit Breakers	22
11. Functional Diagram	10	22.5. Parallel Use to Increase Output Power	23
12. Terminals and Wiring	11	22.6. Parallel Use for Redundancy	23
13. Front Side and User Elements	12	22.7. Series Operation	24
14. EMC	13	22.8. Inductive and Capacitive Loads	24
15. Environment	14	22.9. Charging of Batteries	24
16. Protection Features	15	22.10. Operation on Two Phases	25
17. Safety Features	15	22.11. Use in a Tightly Sealed Enclosure	25
18. Dielectric Strength	16	22.12. Mounting Orientations	26
19. Approvals	17		

The information presented in this document is believed to be accurate and reliable and may change without notice.
No part of this document may be reproduced or utilized in any form without permission in writing from the publisher.

TERMINOLOGY AND ABBREVIATIONS

PE and \oplus symbol	PE is the abbreviation for Protective Earth and has the same meaning as the symbol \oplus .
Earth, Ground	This document uses the term "earth" which is the same as the U.S. term "ground".
T.b.d.	To be defined, value or description will follow later.
AC 230V	A figure displayed with the AC or DC before the value represents a nominal voltage with standard tolerances (usually $\pm 15\%$) included. E.g.: DC 12V describes a 12V battery disregarding whether it is full (13.7V) or flat (10V)
230Vac	A figure with the unit (Vac) at the end is a momentary figure without any additional tolerances included.
50Hz vs. 60Hz	As long as not otherwise stated, AC 230V parameters are valid at 50Hz mains frequency.
may	A key word indicating flexibility of choice with no implied preference.
shall	A key word indicating a mandatory requirement.
should	A key word indicating flexibility of choice with a strongly preferred implementation.

1. INTENDED USE

This device is designed for installation in an enclosure and is intended for the general professional use such as in industrial control, office, communication, and instrumentation equipment.

Do not use this power supply in equipment, where malfunction may cause severe personal injury or threaten human life.

This device is designed for use in hazardous, non-hazardous, ordinary or unclassified locations.

2. INSTALLATION REQUIREMENTS

This device may only be installed and put into operation by qualified personnel.

This device does not contain serviceable parts. The tripping of an internal fuse is caused by an internal defect.

If damage or malfunction should occur during installation or operation, immediately turn power off and send unit to the factory for inspection.

Mount the unit on a DIN-rail so that the terminals are located on the bottom of the unit. For other mounting orientations see de-rating requirements in this document. See chapter 24.13.

This device is designed for convection cooling and does not require an external fan. Do not obstruct airflow and do not cover ventilation grid (e.g. cable conduits) by more than 15%!

Keep the following installation clearances: 40mm on top, 20mm on the bottom, 5mm on the left and right sides are recommended when the device is loaded permanently with more than 50% of the rated power. Increase this clearance to 15mm in case the adjacent device is a heat source (e.g. another power supply).

A disconnecting means shall be provided for the output of the power supplies when used in applications according to CSA C22.2 No 107.1-01.



WARNING Risk of electrical shock, fire, personal injury or death.

- Do not use the power supply without proper grounding (Protective Earth). Use the terminal on the input block for earth connection and not one of the screws on the housing.
- Turn power off before working on the device. Protect against inadvertent re-powering.
- Make sure that the wiring is correct by following all local and national codes.
- Do not modify or repair the unit.
- Do not open the unit as high voltages are present inside.
- Use caution to prevent any foreign objects from entering the housing.
- Do not use in wet locations or in areas where moisture or condensation can be expected.
- Do not touch during power-on, and immediately after power-off. Hot surfaces may cause burns.

Notes for use in hazardous location areas:

The power supply is suitable for use in Class I Division 2 Groups A, B, C, D locations and for use in Group II Category 3 (Zone 2) environments and are evaluated according to EN 60079-0:2012 and EN 60079-15:2010.

WARNING EXPLOSION HAZARDS!

Substitution of components may impair suitability for this environment. Do not disconnect the unit or operate the voltage adjustment or S/P jumper unless power has been switched off or the area is known to be non-hazardous.

A suitable enclosure must be provided for the end product which has a minimum protection of IP54 and fulfils the requirements of the EN 60079-15:2010.

3. AC-INPUT

AC input	nom.	AC 100-240V	suitable for TN-, TT- and IT mains networks
AC input range	min.	100-264Vac	continuous operation
	min.	85-100Vac	short term or with output derating (1%/V) or with reduced ambient temperature, see Fig. 15-1, no damage between 0 and 100Vac
	min.	264-300Vac	< 500ms
Allowed voltage L or N to earth	max.	300Vac	continuous, IEC 62103
Input frequency	nom.	50–60Hz	±6%
Turn-on voltage	typ.	84Vac	steady-state value, see Fig. 3-1
Shut-down voltage	typ.	39Vac	steady-state value at 5A load, see Fig. 3-1
	typ.	53Vac	steady-state value at 10A load, see Fig. 3-1
	typ.	74Vac	steady-state value at 20A load, see Fig. 3-1

		AC 100V	AC 120V	AC 230V	
Input current	typ.	5.25A	4.36A	2.33A	at 24V, 20A, see Fig. 3-3
Power factor ^{*)}	typ.	0.99	0.99	0.95	at 24V, 20A, see Fig. 3-4
Crest factor ^{**)}	typ.	1.5	1.5	1.65	at 24V, 20A
Start-up delay	typ.	850ms	850ms	650ms	see Fig. 3-2
Rise time	typ.	85ms	85ms	85ms	at 24V, 20A const. current load, 0mF load capacitance, see Fig. 3-2
	typ.	150ms	150ms	150ms	at 24V, 20A const. current load, 20mF load capacitance, see Fig. 3-2
Turn-on overshoot	max.	200mV	200mV	200mV	see Fig. 3-2

^{*)} The power factor is the ratio of the true (or real) power to the apparent power in an AC circuit.

^{**)} The crest factor is the mathematical ratio of the peak value to RMS value of the input current waveform.

Fig. 3-1 Input voltage range

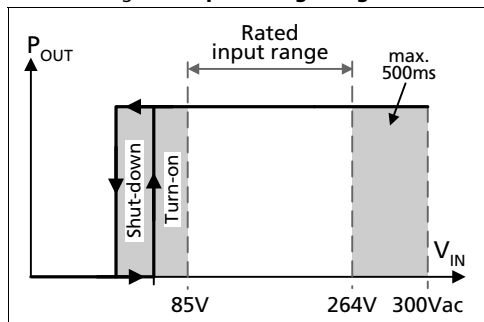


Fig. 3-2 Turn-on behavior, definitions

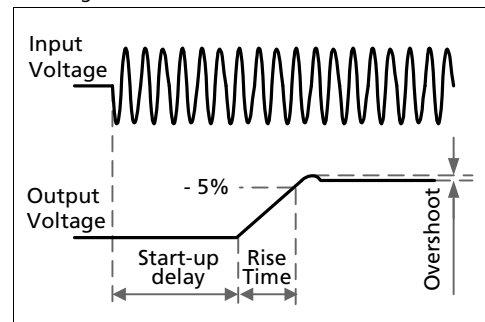


Fig. 3-3 Input current vs. output load at 24V

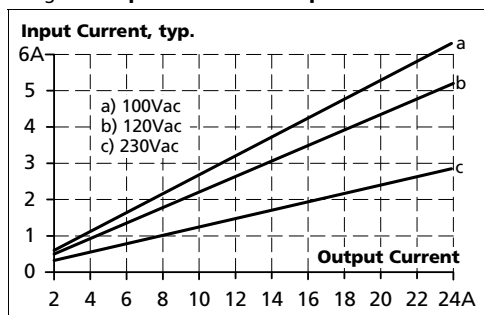
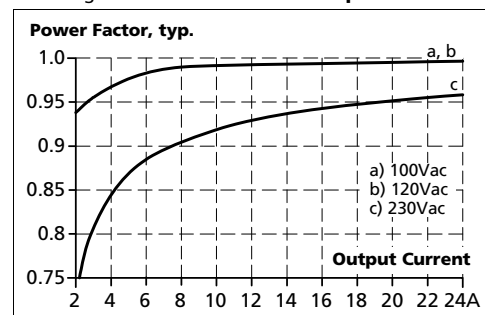


Fig. 3-4 Power factor vs. output load



4. DC-INPUT

Do not operate this power supply with DC-input voltage. Use the CPS20.241-D1 unit instead.

5. INPUT INRUSH CURRENT

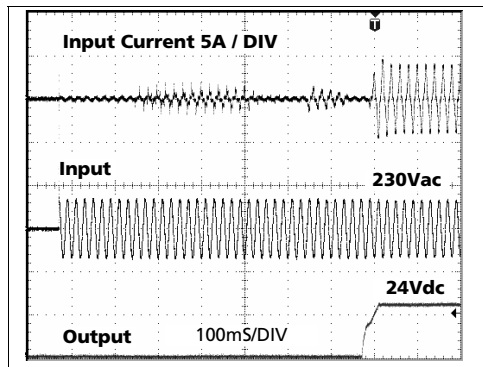
An active inrush limitation circuit limits the input inrush current after turn-on of the input voltage and after short input voltage interruptions.

The charging current into EMI suppression capacitors is disregarded in the first microseconds after switch-on.

		AC 100V	AC 120V	AC 230V	
Inrush current ^{*)}	max.	13A _{peak}	13A _{peak}	13A _{peak}	temperature independent
	typ.	11A _{peak}	9A _{peak}	7A _{peak}	temperature independent
Inrush energy ^{*)}	max.	2A ² s	2.5A ² s	0.5A ² s	temperature independent
Inrush delay	typ.	935ms	935ms	735ms	start-up delay plus rise time

^{*)} Mains interruptions > 500ms

Fig. 5-1 Typical input inrush current behaviour at nominal load and 25°C ambient



6. OUTPUT

Output voltage	nom.	24V	
Adjustment range	min.	24-28V	guaranteed
	max.	30V****)	at clockwise end position of potentiometer
Factory settings	typ.	24.1V	±0.2%, at full load, cold unit, in "single use" mode
	typ.	24.1V	±0.2%, at full load, cold unit, in "parallel use" mode
	typ.	25.1V	at no load, cold unit, in "parallel use" mode
Line regulation	max.	10mV	85-300Vac
Load regulation	max.	100mV	in "single use" mode: static value, 0A → 20A; see Fig. 6-1
	typ.	1000mV	in "parallel use" mode: static value, 0A → 20A, see Fig. 6-2
Ripple and noise voltage	max.	50mVpp	20Hz to 20MHz, 50Ohm
Output current	nom.	20A	at 24V, ambient temperature <60°C, see Fig. 6-1
	nom.	24A*)	at 24V, ambient temperature <45°C, see Fig. 6-1
	nom.	17.1A	at 28V, ambient temperature <60°C, see Fig. 6-1
	nom.	20.6A*)	at 28V, ambient temperature <45°C, see Fig. 6-1
	typ.	80A	up to 15ms, output voltage stays above 20V, see Fig. 6-4, This peak current is available once every five seconds. See chapter 22.1 for more peak current measurements.
Output power	nom.	480W	continuously available
	nom.	576W*)	Power Boost® *)
Overload behaviour		cont. current	output voltage > 13Vdc, see Fig. 6-1
		Hiccup ^{PLUS} mode**)	output voltage < 13Vdc, see Fig. 6-1
Short-circuit current	min.	35A***)	load impedance <10mOhm, see Fig. 6-3
	max.	45A***)	load impedance <10mOhm, see Fig. 6-3
	max.	15A***)	average (R.M.S.) current, load impedance 50mOhm, see Fig. 6-3
	min.	70A	up to 15ms, load impedance <10mOhm, see Fig. 6-4
	typ.	100A	up to 15ms, load impedance <10mOhm, see Fig. 6-4
Output capacitance	typ.	7 000µF	included inside the power supply

*) **Power Boost**

This power/ current is continuously allowed up to an ambient temperature of 45°C.

Above 45°C, do not use this power/ current longer than a duty cycle of 10% and/ or not longer than 1 minute every 10 minutes.

) **Hiccup^{PLUS} Mode

At heavy overloads (when output voltage falls below 13V), the power supply delivers continuous output current for 2s. After this, the output is switched off for approx. 18s before a new start attempt is automatically performed. This cycle is repeated as long as the overload exists. If the overload has been cleared, the device will operate normally. See Fig. 6-3

***)) Discharge current of output capacitors is not included.

****)) This is the maximum output voltage which can occur at the clockwise end position of the potentiometer due to tolerances. It is not guaranteed value which can be achieved. The typical value is about 28.5V (in "single use" mode).

Fig. 6-1 **Output voltage vs. output current, typ.**

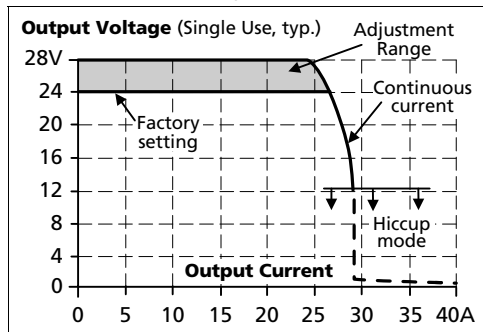


Fig. 6-2 **Output voltage in "parallel use" mode, typ.**

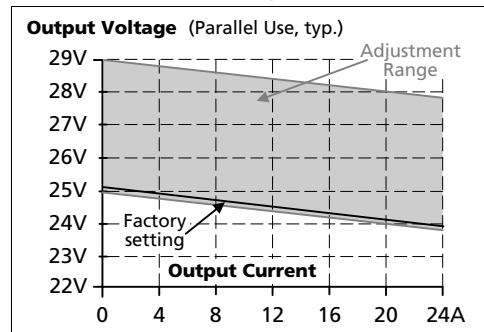


Fig. 6-3 **Short-circuit on output, Hiccup^{plus} mode, typ.**

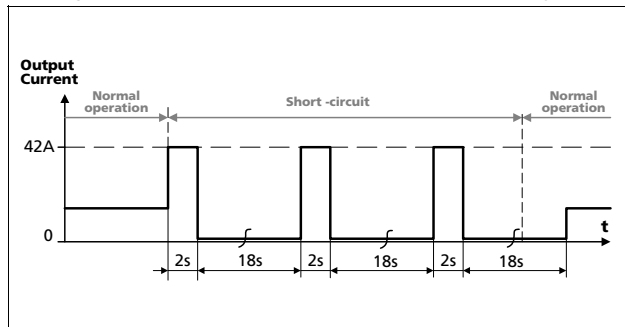
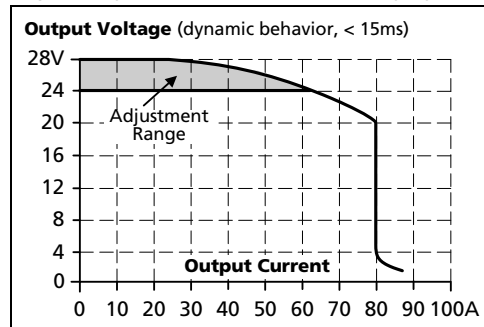


Fig. 6-4 **Dynamic overcurrent capability, typ.**



7. HOLD-UP TIME

		AC 100V	AC 120V	AC 230V	
Hold-up Time	typ.	65ms	65ms	65ms	at 24V, 10A, see Fig. 7-1
	min.	54ms	54ms	54ms	at 24V, 10A, see Fig. 7-1
	typ.	26ms	26ms	26ms	at 24V, 20A, see Fig. 7-1
	min.	21ms	21ms	21ms	at 24V, 20A, see Fig. 7-1

Fig. 7-1 Hold-up time vs. input voltage

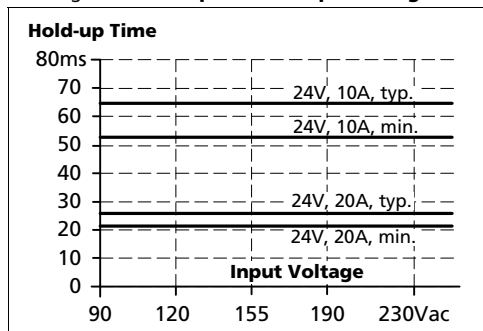
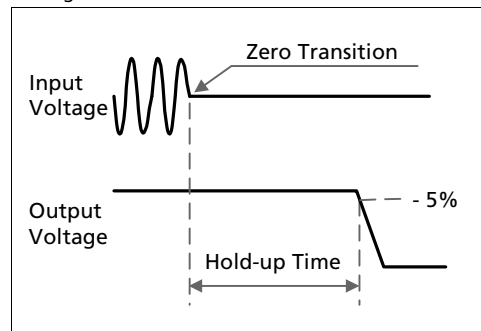


Fig. 7-2 Shut-down behavior, definitions

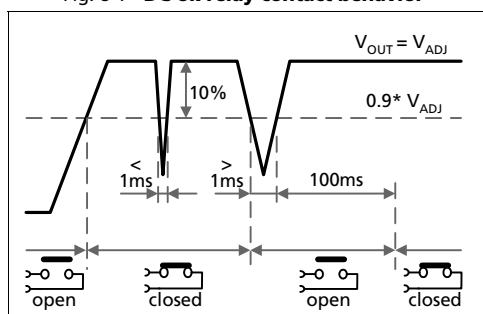


8. DC-OK RELAY CONTACT

This feature monitors the output voltage, which is produced by the power supply itself. It is independent of a back-fed voltage from a unit connected in parallel to the power supply output.

Contact closes	As soon as the output voltage reaches 90% of the adjusted output voltage level.		
Contact opens	As soon as the output voltage dips more than 10% below the adjusted output voltage. Short dips will be extended to a signal length of 100ms. Dips shorter than 1ms will be ignored.		
Contact ratings	max.	60Vdc 0.3A, 30Vdc 1A, 30Vac 0.5A	resistive load
	min.	1mA at 5Vdc	min. permissible load
Isolation voltage	See dielectric strength table in section 18.		

Fig. 8-1 DC-ok relay contact behavior



9. EFFICIENCY AND POWER LOSSES

		AC 100V	AC 120V	AC 230V	
Efficiency	typ.	92.0%	92.7%	94.0%	at 24V, 20A
	typ.	91.6%	92.4%	94.0%	at 24V, 24A (Power Boost)
Average efficiency*)	typ.	91.3%	92.0%	93.3%	25% at 5A, 25% at 10A, 25% at 15A. 25% at 20A
Power losses	typ.	6.5W	3.9W	2.6W	at 24V, 0A
	typ.	21.1W	20.1W	17.0W	at 24V, 10A
	typ.	41.7W	37.8W	30.6W	at 24V, 20A
	typ.	52.8W	47.4W	36.8W	at 24V, 24A (Power Boost)

*) The average efficiency is an assumption for a typical application where the power supply is loaded with 25% of the nominal load for 25% of the time, 50% of the nominal load for another 25% of the time, 75% of the nominal load for another 25% of the time and with 100% of the nominal load for the rest of the time.

Fig. 9-1 Efficiency vs. output current at 24V, typ

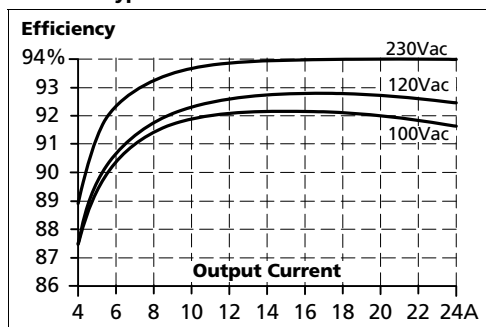


Fig. 9-2 Losses vs. output current at 24V, typ.

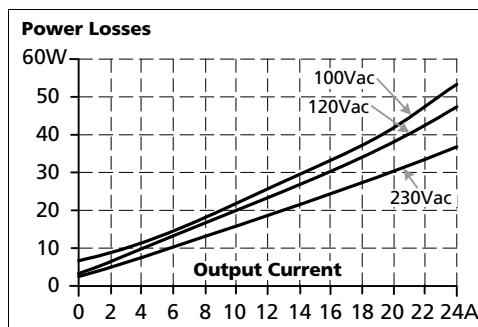


Fig. 9-3 Efficiency vs. input voltage at 24V, 20A, typ.

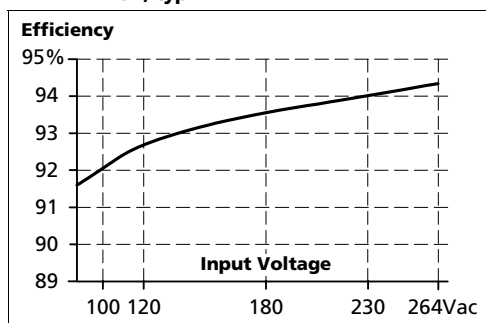
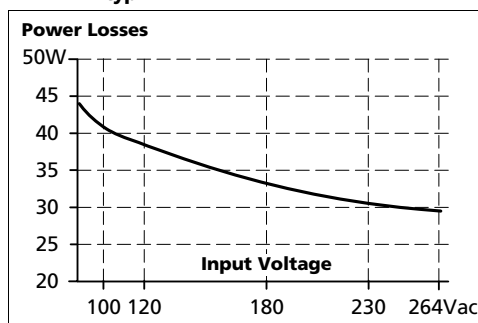


Fig. 9-4 Losses vs. input voltage at 24V, 20A, typ.

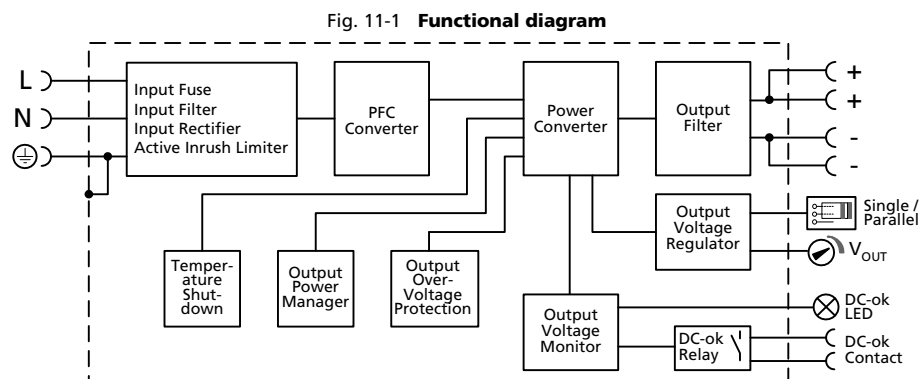


10. LIFETIME EXPECTANCY AND MTBF

	AC 100V	AC 120V	AC 230V	
Lifetime expectancy*)	145 000h*)	150 000h*)	168 000h*)	at 24V, 10A and 40°C
	410 000h*)	425 000h*)	475 000h*)	at 24V, 10A and 25°C
	64 000h	70 000h	88 000h	at 24V, 20A and 40°C
	180 000h*)	198 000h*)	249 000h*)	at 24V, 20A and 25°C
	38 000h	46 000h	61 000h	at 24V, 24A and 40°C
	109 000h*)	130 000h*)	171 000h*)	at 24V, 24A and 25°C
MTBF**) SN 29500, IEC 61709	468 000h	484 000h	537 000h	at 24V, 20A and 40°C
	770 000h	796 000h	882 000h	at 24V, 20A and 25°C
MTBF**) MIL HDBK 217F	254 000h	261 000h	290 000h	at 24V, 20A and 40°C; Ground Benign GB40
	355 000h	361 000h	395 000h	at 24V, 20A and 25°C; Ground Benign GB25
	56 000h	57 000h	64 000h	at 24V, 20A and 40°C; Ground Fixed GF40
	75 000h	77 000h	86 000h	at 24V, 20A and 25°C; Ground Fixed GF25

- *) The **Lifetime expectancy** shown in the table indicates the minimum operating hours (service life) and is determined by the lifetime expectancy of the built-in electrolytic capacitors. Lifetime expectancy is specified in operational hours and is calculated according to the capacitor's manufacturer specification. The manufacturer of the electrolytic capacitors only guarantees a maximum life of up to 15 years (131 400h). Any number exceeding this value is a calculated theoretical lifetime which can be used to compare devices.
- **) **MTBF** stands for **Mean Time Between Failure**, which is calculated according to statistical device failures, and indicates reliability of a device. It is the statistical representation of the likelihood of a unit to fail and does not necessarily represent the life of a product. The MTBF figure is a statistical representation of the likelihood of a device to fail. A MTBF figure of e.g. 1 000 000h means that statistically one unit will fail every 100 hours if 10 000 units are installed in the field. However, it can not be determined if the failed unit has been running for 50 000h or only for 100h.

11. FUNCTIONAL DIAGRAM



12. TERMINALS AND WIRING

The terminals are IP20 Finger safe constructed and suitable for field- and factory wiring.

	Input and output	DC-OK-Signal
Type	screw terminals	spring-clamp terminals
Solid wire	0.5-6mm ²	0.15-1.5mm ²
Stranded wire	0.5-4mm ²	0.15-1.5mm ²
American Wire Gauge	AWG20-10	AWG26-14
Max. wire diameter	2.8mm (including ferrules)	1.5mm (including ferrules)
Wire stripping length	7mm / 0.28inch	7mm / 0.28inch
Screwdriver	3.5mm slotted or cross-head No 2	3.5mm slotted (to open the spring)
Recommended tightening torque	1Nm, 9lb.in	not applicable

Instructions:

- Use appropriate copper cables that are designed for minimum operating temperatures of:
60°C for ambient up to 45°C and
75°C for ambient up to 60°C minimum
90°C for ambient up to 70°C minimum.
- Follow national installation codes and installation regulations!
- Ensure that all strands of a stranded wire enter the terminal connection!
- Do not use the unit without PE connection.
- Unused terminal compartments should be securely tightened.
- Ferrules are allowed.

Daisy chaining:

Daisy chaining (jumping from one power supply output to the next) is allowed as long as the average output current through one terminal pin does not exceed 25A. If the current is higher, use a separate distribution terminal block as shown in Fig. 12-2.

Fig. 12-1 Daisy chaining of outputs

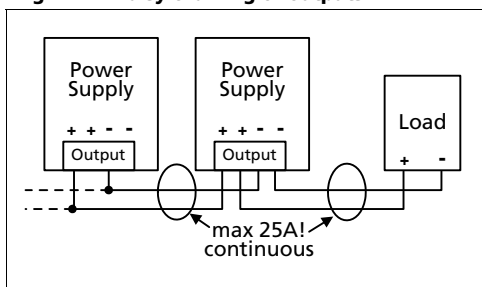
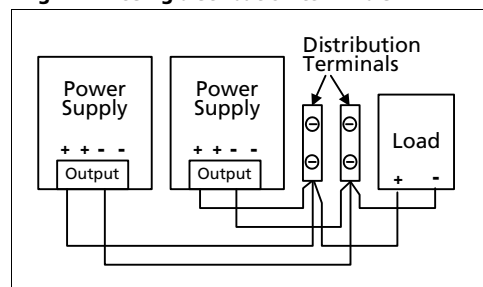
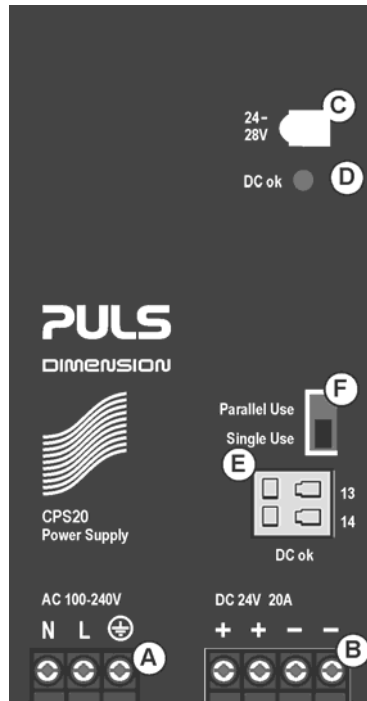


Fig. 12-2 Using distribution terminals



13. FRONT SIDE AND USER ELEMENTS

Fig. 13-1 **Front side**



A Input Terminals (screw terminals)

N, L Line input

⊕ PE (Protective Earth) input

B Output Terminals (screw terminals, two pins per pole)

+ Positive output

- Negative (return) output

C Output voltage potentiometer

Open the flap to adjust the output voltage. Factory set: 24.1V

D DC-OK LED (green)

On, when the output voltage is >90% of the adjusted output voltage

E DC-OK Relay Contact (quick-connect spring-clamp terminals)

The DC-OK relay contact is synchronized with the DC-OK LED. See chapter 8 for details.

F "Parallel Use" "Single Use" selector

Set jumper to "Parallel Use" when power supplies are connected in parallel to increase the output power. In order to achieve a sharing of the load current between the individual power supplies, the "parallel use" regulates the output voltage in such a manner that the voltage at no load is approx. 4% higher than at nominal load. See also chapter 22.5. A missing jumper is equal to a "Single Use" mode.

14. EMC

The power supply is suitable for applications in industrial environment as well as in residential, commercial and light industry environment without any restrictions. A detailed EMC report is available on request.

EMC Immunity		According generic standards: EN 61000-6-1 and EN 61000-6-2		
Electrostatic discharge	EN 61000-4-2	contact discharge	8kV	Criterion A
		air discharge	15kV	Criterion A
Electromagnetic RF field	EN 61000-4-3	80MHz-2.7GHz	20V/m	Criterion A
Fast transients (Burst)	EN 61000-4-4	input lines	4kV	Criterion A
		output lines	2kV	Criterion A
		DC-OK signal (coupling clamp)	2kV	Criterion A
Surge voltage on input	EN 61000-4-5	L → N	2kV	Criterion A
		L → PE, N → PE	4kV	Criterion A
Surge voltage on output	EN 61000-4-5	+ → -	1kV	Criterion A
		+ / - → PE	2kV	Criterion A
Surge voltage on DC-OK	EN 61000-4-5	DC-OK signal → PE	1kV	Criterion A
Conducted disturbance	EN 61000-4-6	0.15-80MHz	20V	Criterion A
Mains voltage dips	EN 61000-4-11	0% of 100Vac	0Vac, 20ms	Criterion A
		40% of 100Vac	40Vac, 200ms	Criterion C
		70% of 100Vac	70Vac, 500ms	Criterion A
		0% of 200Vac	0Vac, 20ms	Criterion A
		40% of 200Vac	80Vac, 200ms	Criterion A
		70% of 200Vac	140Vac, 500ms	Criterion A
Voltage interruptions	EN 61000-4-11	0% of 200Vac (=0V)	5000ms	Criterion C
Voltage sags	SEMI F47 0706	dips on the input voltage according to SEMI F47 standard		
		80% of 120Vac (96Vac)	1000ms	Criterion A
		70% of 120Vac (84Vac)	500ms	Criterion A
		50% of 120Vac (60Vac)	200ms	Criterion A
Powerful transients	VDE 0160	over entire load range	750V, 1.3ms	Criterion A

Criteria:

A: Power supply shows normal operation behavior within the defined limits.

C: Temporary loss of function is possible. Power supply may shut-down and restarts by itself. No damage or hazards for the power supply will occur.

EMC Emission		According generic standards: EN 61000-6-3 and EN 61000-6-4	
Conducted emission input lines	EN 55011, EN 55022, FCC Part 15, CISPR 11, CISPR 22	Class B	
Conducted emission output lines**)	IEC/CISPR 16-1-2, IEC/CISPR 16-2-1	limits for DC power port according EN 61000-6-3 fulfilled	
Radiated emission	EN 55011, EN 55022	Class B	
Harmonic input current	EN 61000-3-2	fulfilled for class A equipment	
Voltage fluctuations, flicker	EN 61000-3-3	fulfilled*)	

This device complies with FCC Part 15 rules.

Operation is subjected to following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

*) tested with constant current loads, non pulsing

**) for information only, not mandatory for EN 61000-6-3

Switching Frequencies	The power supply has two converters with two different switching frequencies included.	
Switching frequency 1	70kHz to 130kHz	PFC converter, input voltage and output power dependent
Switching frequency 2	80kHz to 140kHz	Main converter, output power dependent

15. ENVIRONMENT

Operational temperature ^{*)}	-25°C to +70°C (-13°F to 158°F)	reduce output power according Fig. 15-1
Storage temperature	-40°C to +85°C (-40°F to 185°F)	for storage and transportation
Output de-rating	6.4W/°C 12W/°C	45°C to 60°C (113°F to 140°F) 60°C to 70°C (140°F to 158°F)
Humidity ^{**)}	5 to 95% r.h.	IEC 60068-2-30
Vibration sinusoidal	2-17.8Hz: ±1.6mm; 17.8-500Hz: 2g ^{***)} 2 hours / axis ^{***)}	IEC 60068-2-6
Shock	30g 6ms, 20g 11ms ^{***)} 3 bumps / direction, 18 bumps in total	IEC 60068-2-27
Altitude	0 to 2000m (0 to 6 560ft) 2000 to 6000m (6 560 to 20 000ft)	without any restrictions reduce output power or ambient temperature, see Fig. 15-2
Altitude de-rating	30W/1000m or 5°C/1000m	IEC 62103, EN 50178, overvoltage category II > 2000m (6500ft), see Fig. 15-2
Over-voltage category	III II	IEC 62103, EN 50178, altitudes up to 2000m altitudes from 2000m to 6000m
Degree of pollution	2	IEC 62103, EN 50178, not conductive
LABS compatibility	The unit does not release any silicone or other LABS-critical substances and is suitable for use in paint shops.	
Audible noise	At load currents below 2A some audible noise will be emitted from the power supply	

^{*)} Operational temperature is the same as the ambient or surrounding temperature and is defined as the air temperature 2cm below the unit.

^{**)} Do not energize while condensation is present

^{***)} Tested in combination with DIN-Rails according to EN 60715 with a height of 15mm and a thickness of 1.3mm and standard orientation. Higher levels allowed when using the wall mounting bracket ZM2.WALL

Fig. 15-1 **Output current vs. ambient temp.**

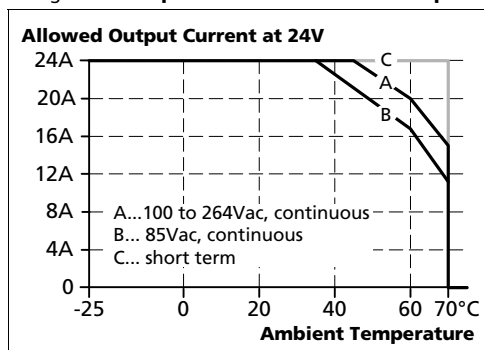
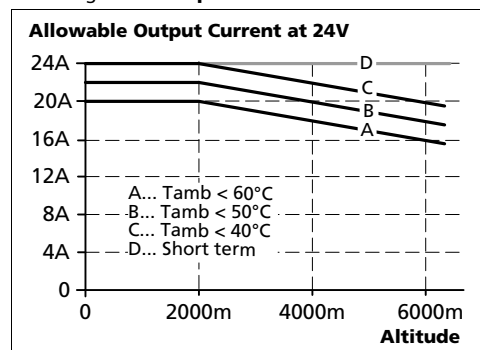


Fig. 15-2 **Output current vs. altitude**



See chapter 3 for de-rating requirements for input voltages between 85Vac and 100Vac.

16. PROTECTION FEATURES

Output protection	Electronically protected against overload, no-load and short-circuits ^{*)}	
Output over-voltage protection	typ. 30.5Vdc max. 32Vdc	In case of an internal power supply defect, a redundant circuit limits the maximum output voltage. The output shuts down and automatically attempts to restart.
Degree of protection	IP 20	EN/IEC 60529 Caution: For use in a controlled environment according to CSA 22.2 No 107.1-01.
Penetration protection	> 5mm	e.g. screws, small parts
Over-temperature protection	yes	Output shut-down with automatic restart
Input transient protection	MOV (Metal Oxide Varistor)	
Internal input fuse	included	not user replaceable

^{*)} In case of a protection event, audible noise may occur.

17. SAFETY FEATURES

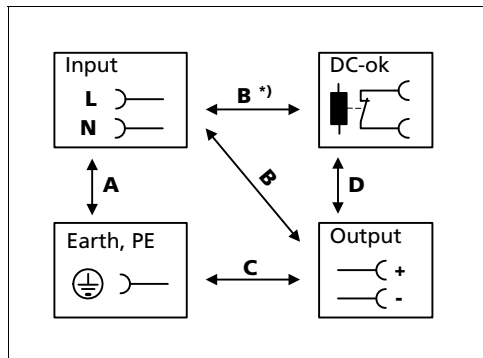
Input / output separation ^{*)}	SELV PELV double or reinforced insulation	IEC/EN 60950-1 IEC/EN 60204-1, EN 50178, IEC 62103, IEC 60364-4-41
Class of protection	I	PE (Protective Earth) connection required
Isolation resistance	> 5MΩ	input to output, 500Vdc
PE resistance	< 0.1Ω	
Touch current (leakage current)	typ. 0.14mA / 0.37mA typ. 0.20mA / 0.55mA typ. 0.35mA / 0.87mA max. 0.17mA / 0.46mA max. 0.26mA / 0.67mA max. 0.46mA / 1.08mA	100Vac, 50Hz, TN-,TT-mains / IT-mains 120Vac, 60Hz, TN-,TT-mains / IT-mains 230Vac, 50Hz, TN-,TT-mains / IT-mains 110Vac, 50Hz, TN-,TT-mains / IT-mains 132Vac, 60Hz, TN-,TT-mains / IT-mains 264Vac, 50Hz, TN-,TT-mains / IT-mains

^{*)} double or reinforced insulation

18. DIELECTRIC STRENGTH

The output voltage is floating and has no ohmic connection to the ground. Type and factory tests are conducted by the manufacturer. Field tests may be conducted in the field using the appropriate test equipment which applies the voltage with a slow ramp (2s up and 2s down). Connect all input-terminals together as well as all output poles before conducting the test. When testing, set the cut-off current settings to the value in the table below.

Fig. 18-1 Dielectric strength



B*) When testing input to DC-OK ensure that the max. voltage between DC-OK and the output is not exceeded (column D). We recommend connecting DC-OK pins and the output pins together when performing the test.

		A	B	C	D
Type test	60s	2500Vac	3000Vac	1000Vac	500Vac
Factory test	5s	2500Vac	2500Vac	500Vac	500Vac
Field test	5s	2000Vac	2000Vac	500Vac	500Vac
Cut-off current setting		> 15mA	> 15mA	> 20mA	> 1mA

To fulfil the PELV requirements according to EN60204-1 § 6.4.1, we recommend that either the + pole, the – pole or any other part of the output circuit shall be connected to the protective earth system. This helps to avoid situations in which a load starts unexpectedly or can not be switched off when unnoticed earth faults occur.

19. APPROVALS

EC Declaration of Conformity



The CE mark indicates conformance with the

- EMC directive 2004/108/EC,
- Low-voltage directive (LVD) 2006/95/EC,
- RoHS directive 2011/65/EU and the
- ATEX directive 94/9/EC (for use in explosive atmospheres)

IEC 60950-1
2nd Edition



CB Scheme,
Information Technology Equipment

UL 508



Listed for use as Industrial Control Equipment;
U.S.A. (UL 508) and Canada (C22.2 No. 107-1-01);
E-File: E198865

UL 60950-1
2nd Edition



Recognized for use as Information Technology Equipment,
Level 5; U.S.A. (UL 60950-1) and Canada (C22.2 No. 60950-1);
E-File: E137006
Applicable for altitudes up to 2000m.

ANSI / ISA 12.12.01-2007
Class I Div 2



Recognized for use in Hazardous Location Class I Div 2 T3
Groups A,B,C,D systems; U.S.A. (ANSI / ISA 12.12.01-2007) and
Canada (C22.2 No. 213-M1987)

EN 60079-0, EN 60079-15
ATEX



Approval for use in hazardous locations Zone 2 Category 3G.
Number of ATEX certificate: EPS 13 ATEX 1 555 X
The power supply must be built-in in an IP54 enclosure.

IEC 60079-0, IEC 60079-15



Suitable for use in Class 1 Zone 2 Groups IIa, IIb and IIc
locations. Number of IECEx certificate: IECEx EPS 13.0016X

Marine



GL (Germanischer Lloyd) classified
Environmental category: C, EMC2
Marine and offshore applications

GOST R



Certificate of Conformity for Russia and other GUS countries

20. PHYSICAL DIMENSIONS AND WEIGHT

Weight	1000g / 2.2lb
DIN-Rail	Use 35mm DIN-rails according to EN 60715 or EN 50022 with a height of 7.5 or 15mm. The DIN-rail height must be added to the unit depth (127mm) to calculate the total required installation depth.
Installation Clearances	See chapter 2

Fig. 20-1 **Front view**

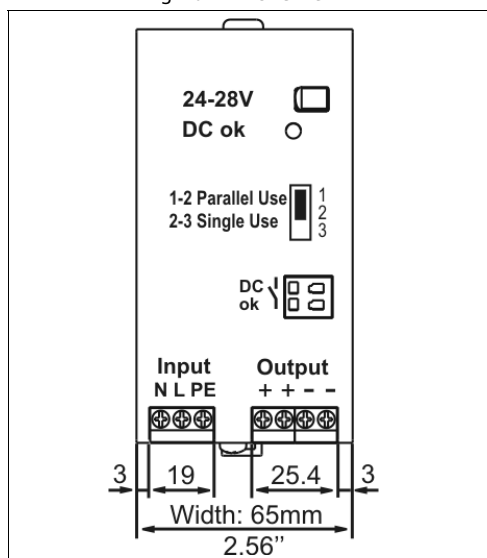
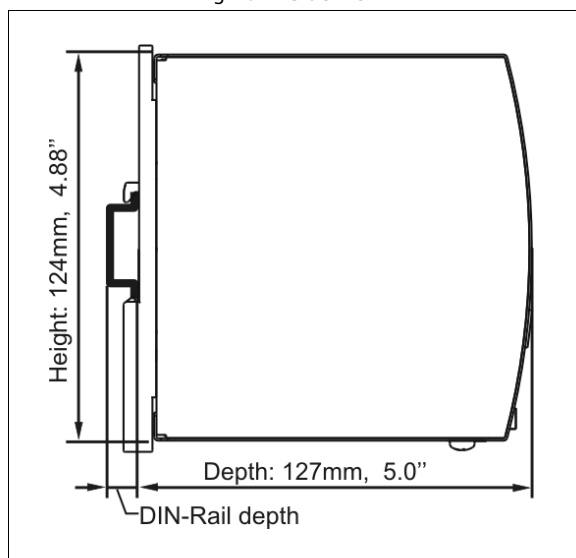


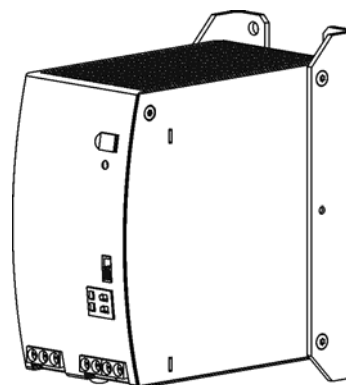
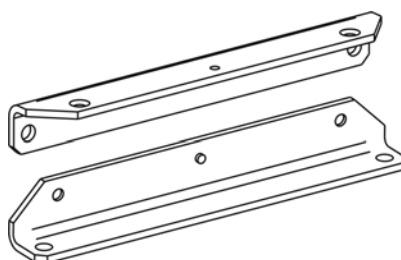
Fig. 20-2 **Side view**



21. ACCESSORIES

21.1. ZM2.WALL - WALL MOUNTING BRACKET

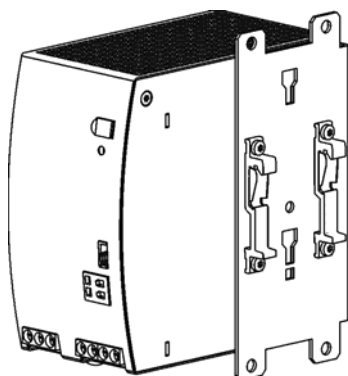
This bracket is used to mount the power supply onto a flat surface without utilizing a DIN-Rail.



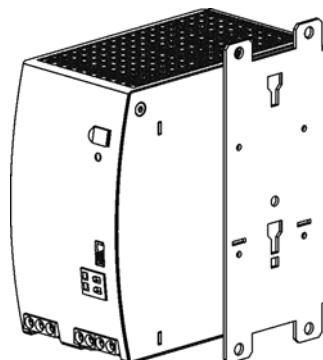
21.2. ZM13.SIDE - SIDE MOUNTING BRACKET

This bracket is used to mount DIMENSION units sideways with or without utilizing a DIN-Rail. The two aluminum brackets and the black plastic slider of the unit have to be detached, so that the steel brackets can be mounted.

For sideways DIN-rail mounting, the removed aluminum brackets and the black plastic slider need to be mounted on the steel bracket.



Side mounting with DIN-rail brackets



Side mounting without DIN-rail brackets

21.3. REDUNDANCY MODULES

YR40.242 – (2x 20A Inputs, 1x 40A output)



The YR40.242 is equipped with two input channels, which are individually decoupled by utilizing mosfet technology. Using mosfets instead of diodes reduces the heat generation and the voltage drop between input and output. The YR40.242 does not require an additional auxiliary voltage and is self-powered even in case of a short circuit across the output.

Due to the low power losses, the unit is very slender and only requires 36mm width on the DIN-rail.

YR40.245 – (1x 40A input, 1x 40A output)



The YR40.245 is a 40A single channel redundancy module, which is equipped with a plug connector on the output. The plug connector allows replacing the power supply or the redundancy module while the system is running. The plug connector avoids that the output wires can touch and short the load circuit.

The YR40.245 is very slender and only requires 46mm width on the DIN-rail. It also utilizes mosfet technology instead of diodes for low heat generation and a minimal voltage drop between input and output. It does not require an additional auxiliary voltage and is self-powered even in case of a short circuit across the output.

Fig. 21-1 Typical 1+1 Redundant configuration for 20A with a dual redundancy module

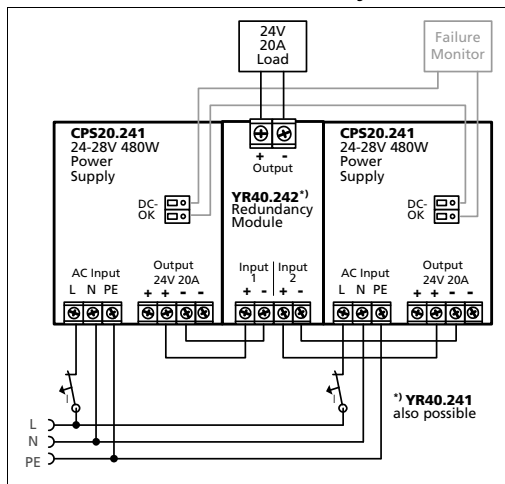
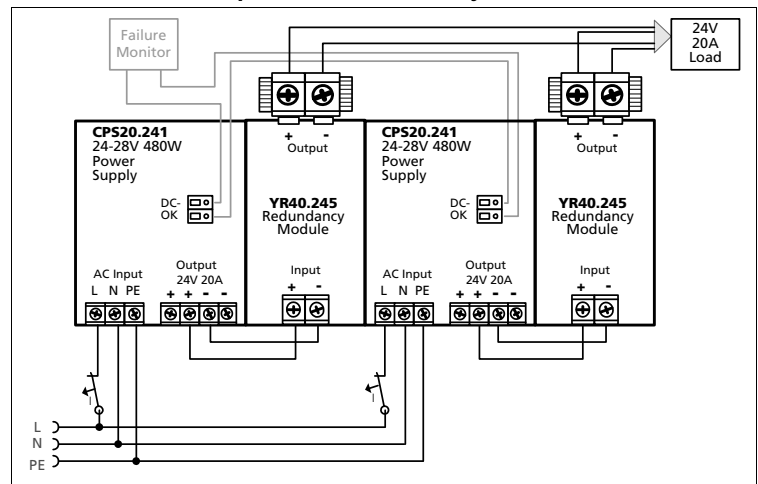


Fig. 21-2 Typical N+1 or 1+1 Redundant configuration for 20A with multiple YR40.245 redundancy modules



22. APPLICATION NOTES

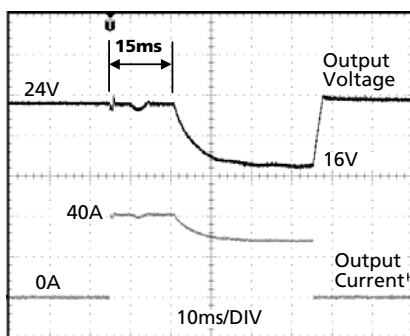
22.1. PEAK CURRENT CAPABILITY

The unit can deliver peak currents (up to several milliseconds) which are higher than the specified short term currents. This helps to start current demanding loads. Solenoids, contactors and pneumatic modules often have a steady state coil and a pick-up coil. The inrush current demand of the pick-up coil is several times higher than the steady-state current and usually exceeds the nominal output current (including the PowerBoost). The same situation applies when starting a capacitive load.

The peak current capability also ensures the safe operation of subsequent circuit breakers of load circuits. The load branches are often individually protected with circuit breakers or fuses. In case of a short or an overload in one branch circuit, the fuse or circuit breaker need a certain amount of over-current to open in a timely manner. This avoids voltage loss in adjacent circuits.

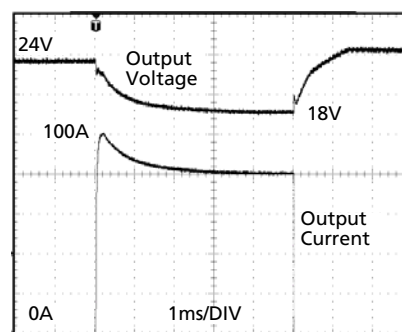
The extra current (peak current) is supplied by the power converter and the built-in large sized output capacitors of the power supply. The capacitors get discharged during such an event, which causes a voltage dip on the output. The following two examples show typical voltage dips:

Fig. 22-1 **Peak load with 2x the nominal current for 50ms, typ.**



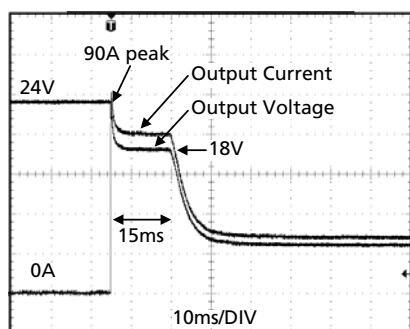
40A Peak load (resistive) for 50ms
Output voltage dips from 24V to 16V.

Fig. 22-2 **Peak load with 5x the nominal current for 5ms, typ.**



100A Peak load (resistive) for 5ms
Output voltage dips from 24V to 18V.

Fig. 22-3 **90A Peak load, typ.**



High Overload Current (typ. >90A for 15ms) enables easy fuse tripping

Please note: The DC-OK relay triggers when the voltage dips more than 10% for longer than 1ms.

Peak current voltage dips	typ.	from 24V to 16V	at 40A for 50ms, resistive load
	typ.	from 24V to 18.5V	at 100A for 2ms, resistive load
	typ.	from 24V to 18V	at 100A for 5ms, resistive load

22.2. BACK-FEEDING LOADS

Loads such as decelerating motors and inductors can feed voltage back to the power supply. This feature is also called return voltage immunity or resistance against Back- E.M.F. (Electro Magnetic Force).

This power supply is resistant and does not show malfunctioning when a load feeds back voltage to the power supply. It does not matter whether the power supply is on or off.

The maximum allowed feed-back-voltage is 35Vdc. The absorbing energy can be calculated according to the built-in large sized output capacitor which is specified in chapter 6.

22.3. EXTERNAL INPUT PROTECTION

The unit is tested and approved for branch circuits up to 30A (UL) and 32A (IEC). An external protection is only required if the supplying branch has an ampacity greater than this. Check also local codes and local requirements. In some countries local regulations might apply.

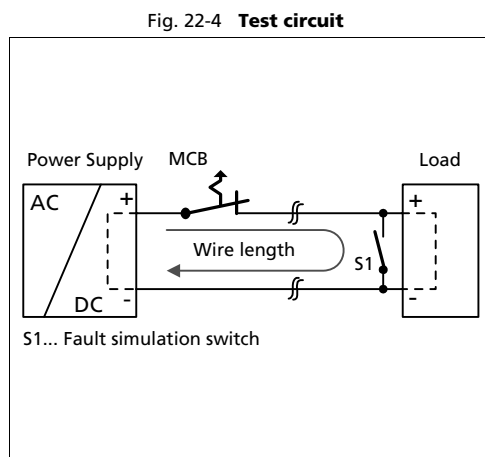
If an external fuse is necessary or utilized, minimum requirements need to be considered to avoid nuisance tripping of the circuit breaker. A minimum value of 10A B- or C-Characteristic breaker should be used.

22.4. OUTPUT CIRCUIT BREAKERS

Standard miniature circuit breakers (MCB's or UL 1077 circuit breakers) are commonly used for AC-supply systems and may also be used on 24V branches.

MCB's are designed to protect wires and circuits. If the ampere value and the characteristics of the MCB are adapted to the wire size that is used, the wiring is considered as thermally safe regardless of whether the MCB opens or not.

To avoid voltage dips and under-voltage situations in adjacent 24V branches which are supplied by the same source, a fast (magnetic) tripping of the MCB is desired. A quick shutdown within 10ms is necessary corresponding roughly to the ride-through time of PLC's. This requires power supplies with high current reserves and large output capacitors. Furthermore, the impedance of the faulty branch must be sufficiently small in order for the current to actually flow. The best current reserve in the power supply does not help if Ohm's law does not permit current flow. The following table has typical test results showing which B- and C-Characteristic MCBs magnetically trip depending on the wire cross section and wire length.



Maximal wire length^{*)} for a fast (magnetic) tripping:

	0.75mm ²	1.0mm ²	1.5mm ²	2.5mm ²
C-2A	29m	40m	56m	82m
C-3A	26m	35m	50m	77m
C-4A	21m	28m	36m	53m
C-6A	8m	10m	14m	25m
C-8A	4m	7m	11m	18m
C-10A	1m	2m	3m	6m
B-6A	17m	24m	35m	53m
B-10A	12m	16m	23m	32m
B-13A	9m	13m	20m	29m
B-16A	4m	7m	9m	17m
B-20A	1m	1m	2m	2m

*) Don't forget to consider twice the distance to the load (or cable length) when calculating the total wire length (+ and - wire).

22.5. PARALLEL USE TO INCREASE OUTPUT POWER

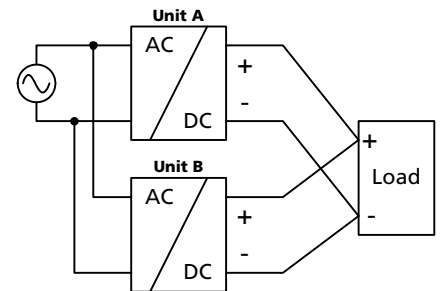
CPS20.241 power supplies can be paralleled to increase the output power. The output voltage of all power supplies shall be adjusted to the same value ($\pm 100\text{mV}$) in "Single use" mode with the same load conditions on all units, or the units can be left with the factory settings. After the adjustments, the jumper on the front of the unit shall be moved from "Single use" to "Parallel use", in order to achieve load sharing. The "Parallel use" mode regulates the output voltage in such a manner that the voltage at no load is approx. 4% higher than at nominal load. See also chapter 6. If no jumper is plugged in, the unit is in "Single use" mode. Factory setting is "Single use" mode.

If more than three units are connected in parallel, a fuse or circuit breaker with a rating of 30A or 32A is required on each output. Alternatively, a diode or redundancy module can also be utilized.

Energize all units at the same time to avoid the overload Hiccup^{PLUS} mode. It also might be necessary to cycle the input power (turn-off for at least five seconds), if the output was in Hiccup^{PLUS} mode due to overload or short circuits and the required output current is higher than the current of one unit.

Keep an installation clearance of 15mm (left / right) between two power supplies and avoid installing the power supplies on top of each other. Do not use power supplies in parallel in mounting orientations other than the standard mounting orientation (terminals on bottom of the unit) or in any other condition where a derating of the output current is required (e.g. altitude, above 60°C, ...).

Pay attention that leakage current, EMI, inrush current, harmonics will increase when using multiple power supplies.



22.6. PARALLEL USE FOR REDUNDANCY

Power supplies can be paralleled for redundancy to gain higher system availability. Redundant systems require a certain amount of extra power to support the load in case one power supply unit fails. The simplest way is to put two power supplies in parallel. This is called a 1+1 redundancy. In case one power supply unit fails, the other one is automatically able to support the load current without any interruption. Redundant systems for a higher power demand are usually built in a N+1 method. E.g. five power supplies, each rated for 20A are paralleled to build a 80A redundant system. For N+1 redundancy the same restrictions apply as for increasing the output power, see also chapter 22.5.

Please note: This simple way to build a redundant system does not cover failures such as an internal short circuit in the secondary side of the power supply. In such a case, the defective unit becomes a load for the other power supplies and the output voltage can not be maintained any more. This can be avoided by utilizing redundancy modules, which have decoupling devices (diodes or mosfets) included. Further information and wiring configurations can be found in chapter 21.3.

Recommendations for building redundant power systems:

- Use separate input fuses for each power supply.
- Set the power supply into "Parallel use" mode.
- Monitor the individual power supply units. Therefore, use the DC-OK relay contact of the CPS20 power supply.
- It is desirable to set the output voltages of all units to the same value ($\pm 100\text{mV}$) or leave it at the factory setting.

22.7. SERIES OPERATION

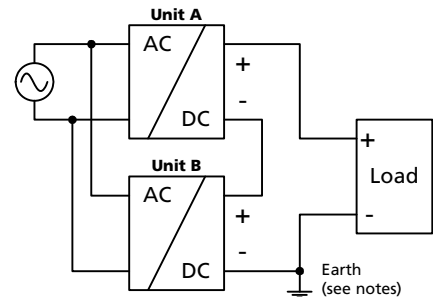
Power supplies of the same type can be connected in series for higher output voltages. It is possible to connect as many units in series as needed, providing the sum of the output voltage does not exceed 150Vdc. Voltages with a potential above 60Vdc are not SELV any more and can be dangerous. Such voltages must be installed with a protection against touching.

Earthing of the output is required when the sum of the output voltage is above 60Vdc.

Avoid return voltage (e.g. from a decelerating motor or battery) which is applied to the output terminals.

Keep an installation clearance of 15mm (left / right) between two power supplies and avoid installing the power supplies on top of each other. Do not use power supplies in series in mounting orientations other than the standard mounting orientation (terminals on bottom of the unit).

Pay attention that leakage current, EMI, inrush current, harmonics will increase when using multiple power supplies.



22.8. INDUCTIVE AND CAPACITIVE LOADS

The unit is designed to supply any kind of loads, including capacitive and inductive loads. If extreme large capacitors, such as EDLCs (electric double layer capacitors or "UltraCaps") with a capacitance > 0.5F are connected to the output, the unit might charge the capacitor in the Hiccup^{PLUS} mode (see chapter 6).

22.9. CHARGING OF BATTERIES

The power supply can be used to charge lead-acid or maintenance free batteries. (Two 12V batteries in series)

Instructions for charging batteries:

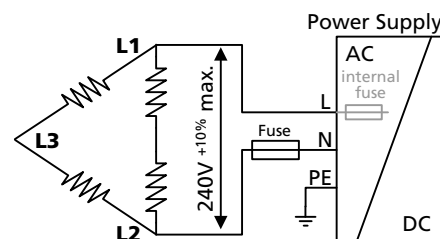
- Set output voltage (measured at no load and at the battery end of the cable) very precisely to the end-of-charge voltage.

End-of-charge voltage	27.8V	27.5V	27.15V	26.8V
Battery temperature	10°C	20°C	30°C	40°C

- Use a 30A or 32A circuit breaker (or blocking diode) between the power supply and the battery.
- Ensure that the output current of the power supply is below the allowed charging current of the battery.
- Use only matched batteries when putting 12V types in series.
- The return current to the power supply (battery discharge current) is typ. 23mA when the power supply is switched off (except in case a blocking diode is utilized).

22.10. OPERATION ON TWO PHASES

The power supply can also be used on two-phases of a three-phase-system. Such a phase-to-phase connection is allowed as long as the supplying voltage is below $240V^{+10\%}$.



22.11. USE IN A TIGHTLY SEALED ENCLOSURE

When the power supply is installed in a tightly sealed enclosure, the temperature inside the enclosure will be higher than outside. In such situations, the inside temperature defines the ambient temperature for the power supply.

The following measurement results can be used as a reference to estimate the temperature rise inside the enclosure.

The power supply is placed in the middle of the box, no other heat producing items are inside the box

Enclosure:	Rittal Typ IP66 Box PK 9522 100, plastic, 254x180x165mm
Load:	24V, 16A; (=80%) load is placed outside the box
Input:	230Vac
Temperature inside enclosure:	53.5°C (in the middle of the right side of the power supply with a distance of 2cm)
Temperature outside enclosure:	25.3°C
Temperature rise:	28.2K

22.12. MOUNTING ORIENTATIONS

Mounting orientations other than all terminals on the bottom require a reduction in continuous output power or a limitation in the maximum allowed ambient temperature. The amount of reduction influences the lifetime expectancy of the power supply. Therefore, two different derating curves for continuous operation can be found below:

Curve A1

Recommended output current.

Curve A2

Max allowed output current (results in approximately half the lifetime expectancy of A1).

Fig. 22-5
Mounting Orientation A
(Standard orientation)

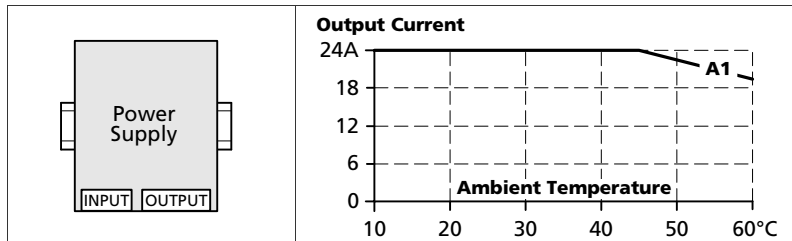


Fig. 22-6
Mounting Orientation B
(Upside down)

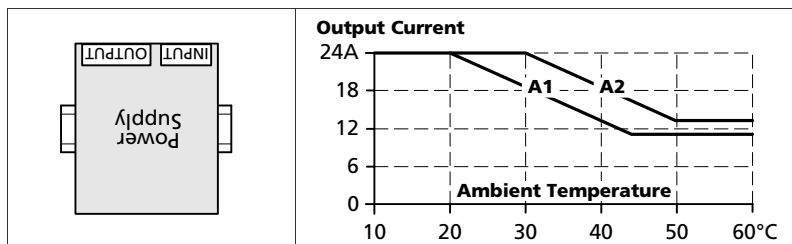


Fig. 22-7
Mounting Orientation C
(Table-top mounting)

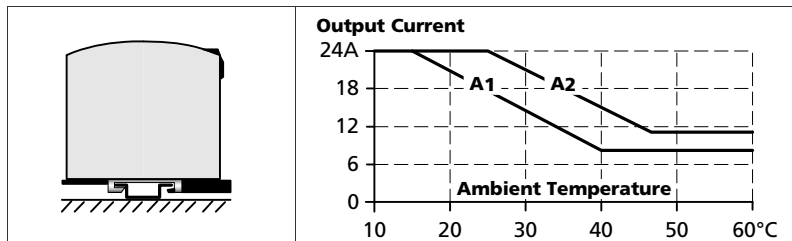


Fig. 22-8
Mounting Orientation D
(Horizontal cw)

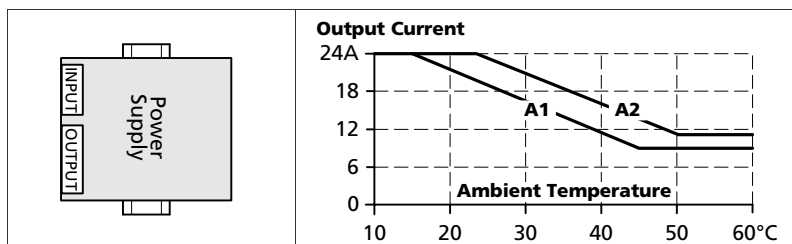
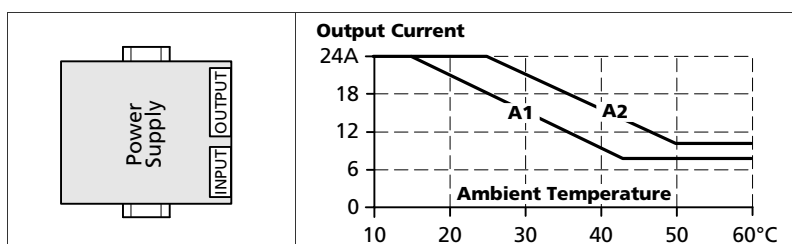
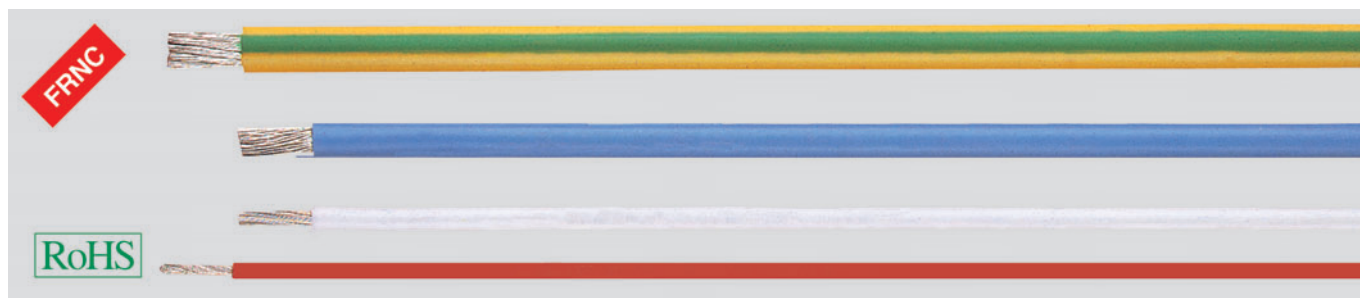


Fig. 22-9
Mounting Orientation E
(Horizontal ccw)





Technical data

- Halogen-free single cores with increased heat resistance
- **Temperature range**
flexing -35 °C to +120 °C
fixed installation -55 °C to +145 °C
- **Nominal voltage**
U₀/U 300/500 V up to 1 mm²
U₀/U 450/ 750 V from 1,5 mm²
for fixed and protected installation
U₀/U 600/1000 V from 1,5 mm²
- **Test voltage** 3500 V
- **Minimum bending radius**
flexing 12,5x cable ø
fixed installation 4x cable ø
- **Caloric load values**
see Technical Informations
- **Power ratings table**
see Technical Informations
- **Approval**
Germanischer Lloyd

Cable structure

- Tinned Cu wires, according to DIN VDE 0295 cl. 5, BS 6360 cl. 5 and IEC 60228 cl. 5
- Core insulation of polyolefin-copolymer, cross-linked
- Core colours see table

Tests

- **Flame test (unit flame test)** to VDE 0482-332-3, BS 4066 part 3/ DIN EN 60332-3-22, IEC 60332-3-22 (equivalent DIN VDE 0472 part 804 test method C)
- **Flame test (cable)** to VDE 0482-332-1-2, DIN EN 60332-1-2, IEC 60332-1-2 (equivalent DIN VDE 0472 part 804 test method B)
- **Corrosiveness of combustion gases** according to VDE 0482 part 267/ DIN EN 50267-2-2/ IEC 60754-2 (equivalent DIN VDE 0472 part 813)
- **Halogen-free** according to VDE 0482 part 267/ DIN EN 50267-2-1/ IEC 60754-1 (equivalent DIN VDE 0472 part 815)
- **Smoke density** to VDE 0482 part 268-1 and 2, test method C, IEC 61034-1/61034-2, HD 606 and BS 7622 part 1 and 2 (DIN VDE 0472 part 816)

Properties

- Lower propagation of fire
- Low development of smoke and fumes
- Good abrasion and notch resistance
- Good resistance to oils and weathering
- Resistant to UV radiation and ozone
- Resistant to soldering temperatures
- Thermal class B
- These single-core cables are resistant to melting, even when in contact with a soldering iron at temperatures of between 300 °C and 380 °C, because of the cross-linking for the insulation material
- Due to the high temperature profile the cross-section of conductor can under certain circumstances be reduced, hereby enabling a saving in space requirement and weight
- The materials used in manufacture are cadmium-free and contain no silicone and free from substances harmful to the wetting properties of lacquers

K

Application

These temperature resistant single-core cables are used for the internal wiring of lighting fixtures, heaters, electrical machinery, switching systems and distributors in equipment and plant and machinery, suitable for installation on, in and beneath plaster, in closed installation ducts, as well as for traffic systems and outdoor applications. These cables are not approved for direct routing on racks, gutters or tanks. For a protected installation, these cables may be used at a nominal voltage of up to 1000 V alternating current or a direct current up to 750 V when earthed. The maximum operating d.c. voltage used in rail vehicles shall not exceed 900 V when earthed. These halogen-free single core cables are characterised by their amazingly high long-time resistance to temperature and feature among the leading halogen-free, flame resistant products in the world. These single core cables significantly contribute to safety and the environment.

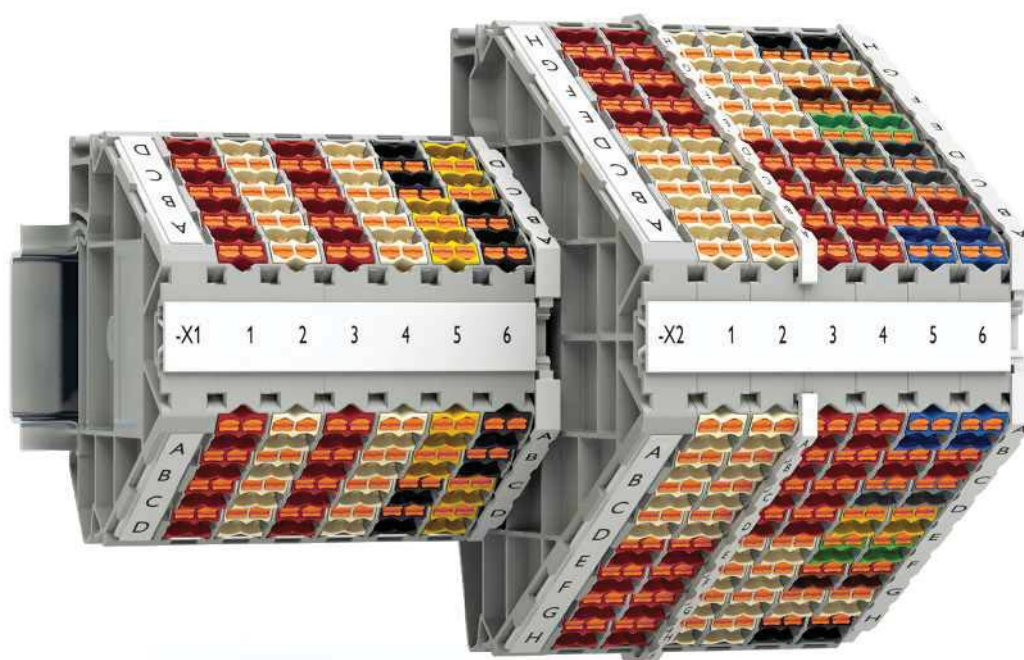
CE The product is conformed with the EC Low-Voltage Directive 2006/95/EG.

Cross-section mm ² approx. RAL	Outer Ø min. - max. mm	Cop. weight kg / km	Weight approx. kg / km	black	gn-ye	brown	red	white	grey	vio	dk-bu	ye	Beige	lt-bu	og	green	2-col.
Part no. 0,25	1,4 - 1,8	2,4	4,0	50999	50998	51071	51072	51073	51074	51075	51079	51076	51164	51070	51077	51078	51165
Part no. 0,33	1,5 - 1,9	3,2	5,0	51167	51166	51169	51170	51171	51172	51173	51177	51174	51178	51168	51175	51176	51179
Part no. 0,5	1,7 - 2,1	4,8	7,0	51281	51280	51283	51284	51285	51286	51287	51291	51288	51292	51282	51289	51290	51293
Part no. 0,75	2,0 - 2,4	7,2	11,0	51295	51294	51297	51298	51299	51300	51301	51305	51302	51306	51296	51303	51304	51307
Part no. 1	2,3 - 2,7	9,6	14,0	51309	51308	51311	51312	51313	51314	51315	51319	51316	51320	51310	51317	51318	51321
Part no. 1,5	2,7 - 3,1	14,4	20,0	51323	51322	51325	51326	51327	51328	51329	51333	51330	51334	51324	51331	51332	51335
Part no. 2,5	3,3 - 3,7	24,0	30,0	51337	51336	51339	51340	51341	51342	51343	51347	51344	51348	51338	51345	51346	51349
Part no. 4	4,1 - 4,5	38,0	47,0	51351	51350	51353	51354	51355	51356	51357	51361	51358	51362	51352	51359	51360	51363
Part no. 6	4,75 - 5,25	58,0	72,0	51365	51364	51367	51368	51369	51370	51371	51375	51372	51376	51366	51373	51374	51377
Part no. 10	6,0 - 6,6	96,0	120,0	51379	51378	51381	51382	51383	51384	51385	51389	51386	51390	51380	51387	51388	51391

Continuation ►

Terminal Blocks

2015/2016





Terminal blocks



Sensor/actuator cabling and industrial connectors

- Sensor/actuator cabling
- Cables and lines
- Connectors



Interface technology and switching devices

- Electronic switching devices and motor control
- Measurement and control technology
- Monitoring
- Relay modules
- System cabling for controllers



Marking systems, tools, and mounting material

- Marking and labeling
- Tools
- Installation and mounting material



Control technology, I/O systems, and automation infrastructure

- Lighting and signaling
- Fieldbus components and systems
- Functional Safety
- HMIs and industrial PCs
- I/O systems
- Industrial Ethernet
- Industrial communication technology
- Software
- Controllers
- Wireless data communication



Surge protection and power supplies

- Surge protection and interference suppression filters
- Power supplies and UPS
- Protective devices



PCB connection technology and electronics housing 2013/14

- PCB terminal blocks and PCB connectors
- Electronics housing

Connection technology for field devices 2013/14

- Connectors
- Cables and lines

Find out more with the web code

On some of the catalog pages, you can find our web codes: a number sign followed by a four-digit number combination.



Web code: #1234 (example)

This allows you to reach information on our website quickly.

It couldn't be simpler:

1. Go to the Phoenix Contact website
2. Enter # and the number combination in the search field
3. Receive more information and product versions

Or use the direct link:

phoenixcontact.net/webcode/#1234

Information on these products can be found in the electronic product catalogs for 2013/14.

Or get the latest on all the new products and additional information directly in the product area of our website:

phoenixcontact.net/products



Also discover the Phoenix Contact catalog app interactively on your tablet.

Table of contents

Product range overview in pictures

4

From here, you can access the desired product directly

System features

15

CLIPLINE complete

UT... screw connection terminal blocks



25

PT... push-in connection terminal blocks



79

ST... spring-cage connection terminal blocks



161

Terminal blocks

CLIPLINE complete

QT... fast connection terminal blocks



209

COMBI plug-in connection solutions



225

RT... bolt connection terminal blocks



323

Accessories



337

Terminal blocks

UK... universal terminal blocks



357

SK... shield terminals



Sector-specific solutions



525

Services

Terminal strips, CLIPSAFE terminal boxes, planning and marking software



589

Technical information and index

598

Product range in pictures

From here, you can access the desired product directly

UT... screw connection terminal blocks



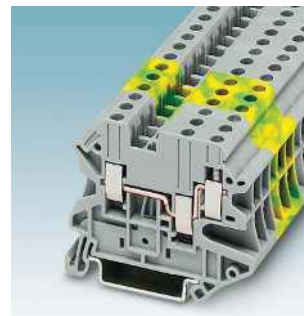
Page 25



Feed-through, multi-conductor, and multi-level terminal blocks and ground terminals
2.5 mm² ... Page 30
4 mm² ... Page 40
6 mm² ... Page 52



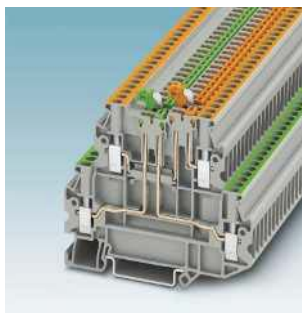
10 mm² ... Page 60
16 mm² ... Page 62
35 mm² ... Page 64
50 mm² - 240 mm² Page 66



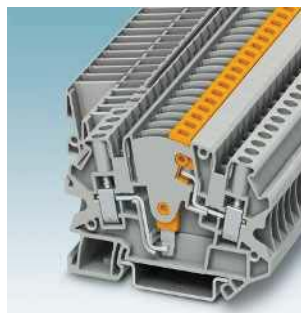
Three-conductor terminal blocks
2.5 mm² ... Page 31
4 mm² ... Page 41



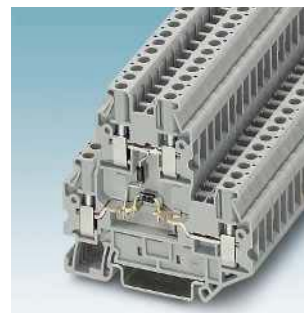
Disconnect terminal blocks
2.5 mm² ... Page 33
4 mm² ... Page 45
6 mm² ... Page 54



Knife disconnect terminal blocks
2.5 mm² ... Page 34
4 mm² ... Page 47
6 mm² ... Page 55



Test disconnect terminal blocks
4 mm² ... Page 49
6 mm² ... Page 56



Diode terminal blocks
2.5 mm² ... Page 35
4 mm² ... Page 50

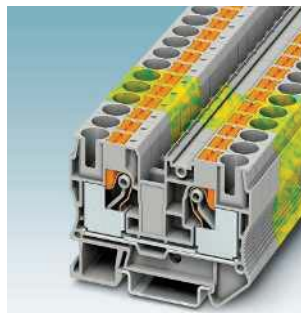
PT... push-in connection terminal blocks



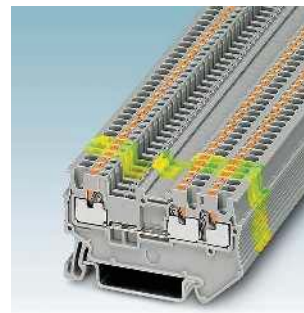
Page 79



Feed-through, multi-conductor, and multi-level terminal blocks and ground terminals
1.5 mm² ... Page 86
2.5 mm² ... Page 110
4 mm² ... Page 132
6 mm² ... Page 140



10 mm² ... Page 146
16 mm² ... Page 148



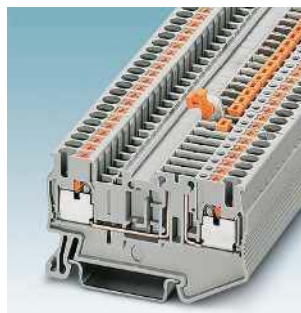
Three-conductor terminal blocks
1.5 mm² ... Page 87
2.5 mm² ... Page 111
4 mm² ... Page 133
6 mm² ... Page 141



Initiator/actuator terminal blocks
2.5 mm² ... Page 89



Fuse terminal blocks
4 mm² ... Page 134
10 mm² ... Page 147



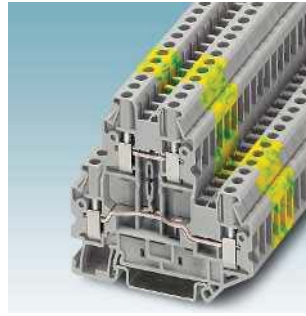
Disconnect and knife disconnect terminal blocks
1.5 mm² ... Page 90
2.5 mm² ... Page 113
4 mm² ... Page 135



Test disconnect terminal blocks
4 mm² ... Page 136
6 mm² ... Page 142



Four-conductor terminal blocks
2.5 mm² ... Page 31
4 mm² ... Page 41



Double-level terminal blocks
2.5 mm² ... Page 31
4 mm² ... Page 42



Three-level terminal blocks
2.5 mm² ... Page 32
4 mm² ... Page 42



Fuse terminal blocks
4 mm² ... Page 43
6 mm² ... Page 53



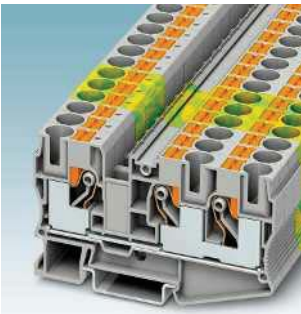
Installation terminal blocks
2.5 mm² ... Page 36
4 mm² ... Page 51
6 mm² ... Page 58
10 mm² ... Page 61



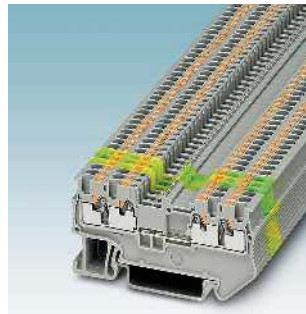
16 mm² ... Page 63
35 mm² ... Page 65



Mini feed-through terminal blocks and
ground terminals
2.5 mm² ... Page 39
4 mm² ... Page 51



10 mm² ... Page 147
16 mm² ... Page 149



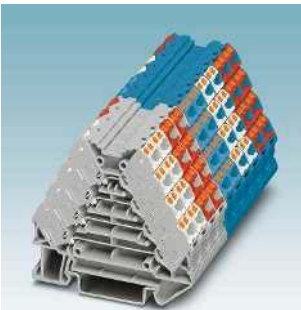
Four-conductor terminal blocks
1.5 mm² ... Page 87
2.5 mm² ... Page 111
4 mm² ... Page 133
6 mm² ... Page 141



Double-level terminal blocks
1.5 mm² ... Page 87
2.5 mm² ... Page 111
4 mm² ... Page 133



Three-level terminal blocks
1.5 mm² ... Page 88
2.5 mm² ... Page 112



Marshall terminals
2.5 mm² ... Page 92



Marshall patchboards
2.5 mm² ... Page 99



Diode terminal blocks
2.5 mm² ... Page 121
4 mm² ... Page 137



Hybrid terminal blocks with single-sided
screw connection
2.5 mm² ... Page 123
4 mm² ... Page 137
16 mm² ... Page 123

Product range in pictures

From here, you can access the desired product directly



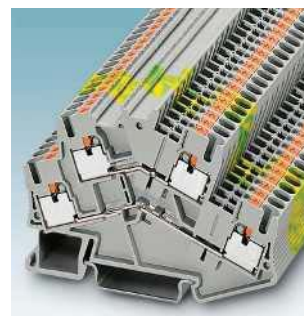
Feed-through terminal blocks and ground terminals, desk design
1.5 mm² ... Page 108
2.5 mm² ... Page 124



Three-conductor terminal blocks, desk design
1.5 mm² ... Page 108
2.5 mm² ... Page 124



Four-conductor terminal blocks, desk design
1.5 mm² ... Page 108
2.5 mm² ... Page 124

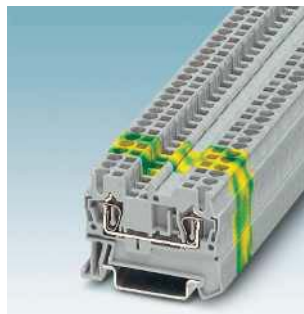


Double-level terminal blocks, desk design
1.5 mm² ... Page 108
2.5 mm² ... Page 124

ST... spring-cage connection terminal blocks



Page 161



Feed-through, multi-conductor, and multi-level terminal blocks and ground terminals
1.5 mm² ... Page 166
2.5 mm² ... Page 170
4 mm² ... Page 186



6 mm² ... Page 194
10 mm² ... Page 200
16 mm² ... Page 204
35 mm² ... Page 206



Three-conductor terminal blocks
1.5 mm² ... Page 167
2.5 mm² ... Page 171
4 mm² ... Page 187
6 mm² ... Page 195



Initiator/actuator terminal blocks
2.5 mm² ... Page 174



Fuse terminal blocks
4 mm² ... Page 189
6 mm² ... Page 199



Disconnect and knife disconnect terminal blocks
2.5 mm² ... Page 176
4 mm² ... Page 190



Test disconnect terminal blocks
6 mm² ... Page 195



Three-conductor terminal blocks, desk design
2.5 mm² ... Page 180
4 mm² ... Page 191
6 mm² ... Page 197



Four-conductor terminal blocks, desk design
2.5 mm² ... Page 181
4 mm² ... Page 192

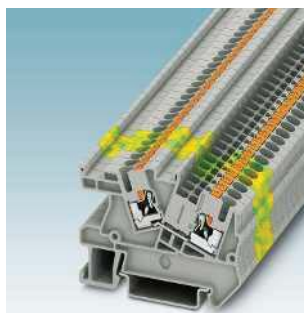


Double-level terminal blocks, desk design
2.5 mm² ... Page 181
4 mm² ... Page 192



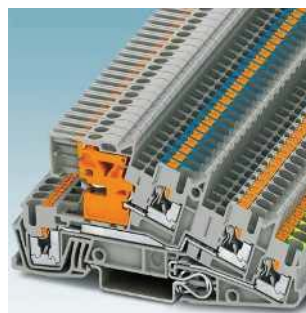
Disconnect and knife disconnect terminal blocks, desk design
2.5 mm² ... Page 181
4 mm² ... Page 193

PTPOWER



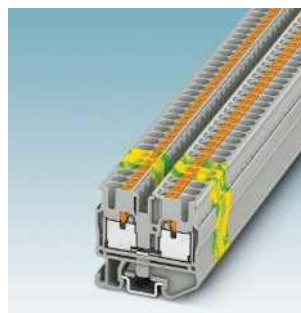
Installation terminal blocks
2.5 mm² ...
4 mm² ...
6 mm² ...

Page 126
Page 138
Page 145



Multi-level installation terminal blocks
2.5 mm² ...
4 mm² ...

Page 127
Page 139



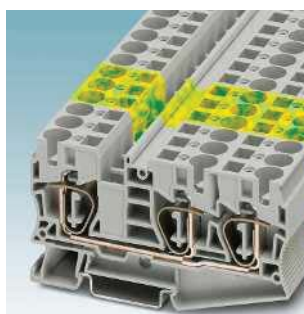
Mini feed-through terminal blocks and
ground terminals
1.5 mm² ...
2.5 mm² ...

Page 109
Page 131



High-current terminal blocks and high-
current terminal block bases
35 mm² ...
50 mm² ...
95 mm² ...
150 mm² ...

Page 153
Page 155
Page 157
Page 159



10 mm² ...
16 mm² ...

Page 201
Page 205



Four-conductor terminal blocks
1.5 mm² ...
2.5 mm² ...
4 mm² ...

Page 167
Page 171
Page 187



Double-level terminal blocks
1.5 mm² ...
2.5 mm² ...
4 mm² ...

Page 168
Page 172
Page 188



Three-level terminal blocks
2.5 mm² ...

Page 173



Diode terminal blocks
2.5 mm² ...
4 mm² ...

Page 178
Page 190



Double-level diode terminal blocks
2.5 mm² ...

Page 178



Hybrid terminal blocks with single-sided
screw connection
2.5 mm² ...
4 mm² ...
10 mm² ...
35 mm² ...

Page 180
Page 191
Page 202
Page 207



Feed-through terminal blocks and ground
terminals, desk design
2.5 mm² ...
4 mm² ...
6 mm² ...

Page 180
Page 191
Page 197



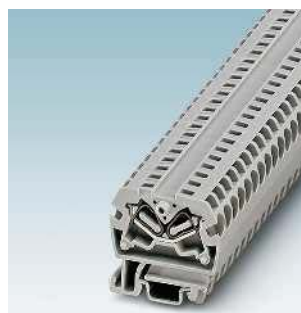
Installation terminal blocks
10 mm² ...
16 mm² ...
35 mm² ...

Page 201
Page 205
Page 207



Mini feed-through terminal blocks and
ground terminals, with vertical conductor exit
2.5 mm² ...

Page 182



Mini feed-through terminal blocks and
ground terminals, with horizontal conductor
exit
2.5 mm² ...

Page 184

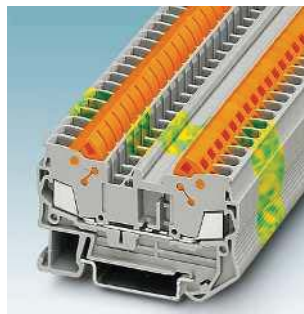
Product range in pictures

From here, you can access the desired product directly

QT... fast connection terminal blocks



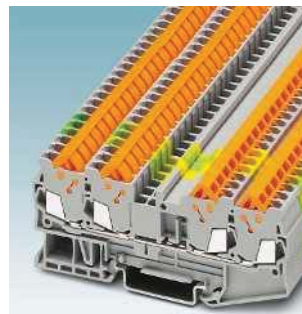
Page 209



Feed-through and multi-conductor terminal blocks
1.5 mm² ... Page 214
2.5 mm² ... Page 220

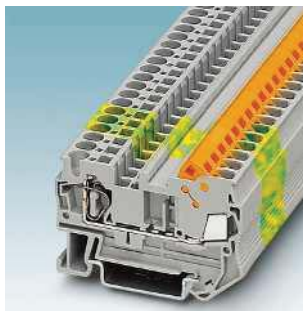


Three-conductor terminal blocks
1.5 mm² ... Page 215
2.5 mm² ... Page 221



Four-conductor terminal blocks
1.5 mm² ... Page 215
2.5 mm² ... Page 221

COMBI plug-in connection solutions



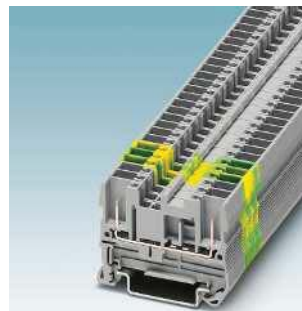
Hybrid terminal blocks with spring-cage connection on one side
1.5 mm² ... Page 219
2.5 mm² ... Page 223



Page 225



Feed-through, multi-conductor, and multi-level terminal blocks and ground terminals with screw connection
2.5 mm² ... Page 234
4 mm² ... Page 240
6 mm² ... Page 250



Terminal blocks that can be connected on both sides
2.5 mm² ... Page 236
4 mm² ... Page 242



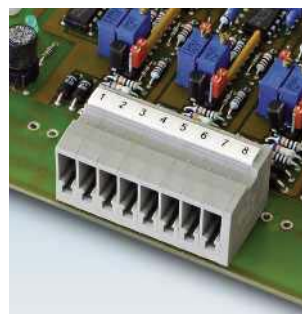
Terminal blocks that can be connected on both sides
1.5 mm² ... Page 256
2.5 mm² ... Page 265
4 mm² ... Page 271



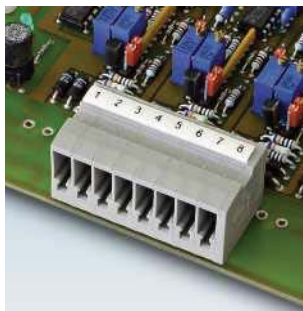
Test disconnect terminal blocks
6 mm² ... Page 275



Couplings with push-in connection - assembled and for self-assembly
1.5 mm² ... Page 258
6 mm² ... Page 278



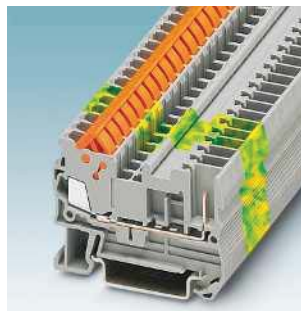
Headers
2.5 mm² ... Page 267
4 mm² ... Page 272



Headers
2.5 mm² ... Page 291
4 mm² ... Page 304



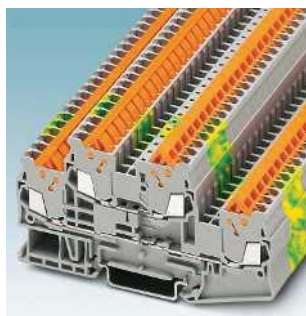
Connectors with spring-cage connection - assembled and for self-assembly
2.5 mm² ... Page 292
4 mm² ... Page 305



Feed-through and multi-level terminal blocks and ground terminals with fast connection
1.5 mm² ... Page 306



Connectors with fast connection - assembled and for self-assembly
1.5 mm² ... Page 308



Double-level terminal blocks
1.5 mm² ...

Page 216



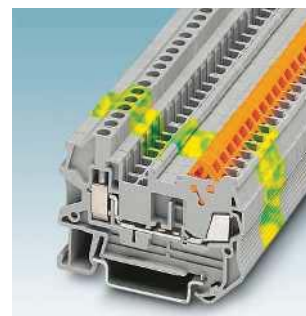
Fuse terminal blocks
2.5 mm² ...

Page 222



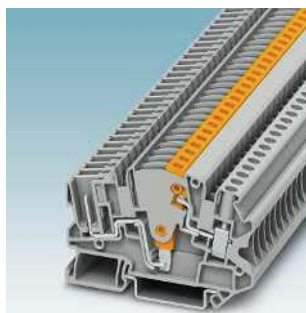
Disconnect and knife disconnect terminal blocks
1.5 mm² ...

Page 216



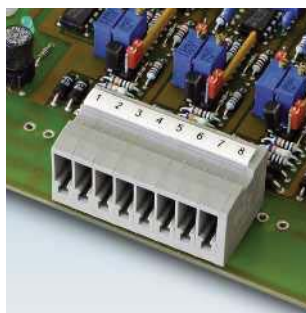
Hybrid terminal blocks with single-sided screw connection
1.5 mm² ...
2.5 mm² ...

Page 218
Page 222



Test disconnect terminal blocks
4 mm² ...

Page 243



Headers
2.5 mm² ...
4 mm² ...

Page 237
Page 245



Connectors with screw connection - assembled and for self-assembly
2.5 mm² ...
4 mm² ...
6 mm² ...

Page 238
Page 247
Page 252



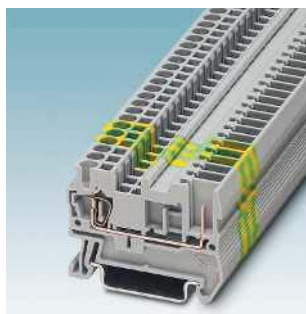
Feed-through, multi-conductor, and multi-level terminal blocks and ground terminals with push-in connection
1.5 mm² ...
2.5 mm² ...
4 mm² ...
6 mm² ...

Page 254
Page 262
Page 270
Page 274



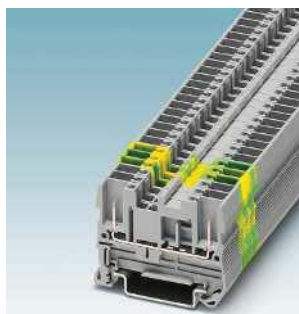
Connectors with push-in connection - assembled and for self-assembly
1.5 mm² ...
2.5 mm² ...
4 mm² ...
6 mm² ...

Page 260
Page 268
Page 273
Page 280



Feed-through, multi-conductor, and multi-level terminal blocks and ground terminals with spring-cage connection
2.5 mm² ...
4 mm² ...

Page 282
Page 298



Terminal blocks that can be connected on both sides
2.5 mm² ...
4 mm² ...

Page 286
Page 299



Couplings with spring-cage connection - assembled and for self-assembly
2.5 mm² ...
4 mm² ...

Page 287
Page 301



Latching and strain relief
PR ..., PRZ ...

Page 313



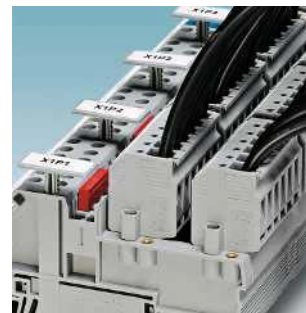
Latching
PR ..., UPR ...

Page 313



Cable housing for COMBI connectors
PH ...

Page 316



Self-locking flange covers
DFS ...
Screw flange and flange cover
UP ...-F

Page 319
Page 320

Product range in pictures

From here, you can access the desired product directly

RT... bolt connection terminal blocks



Page 323



Feed-through terminal blocks

2.5 mm² ...

6 mm² ...

35 mm² ...

Page 328

Page 330

Page 334



Feed-through terminal blocks, open design

2.5 mm² ...

6 mm² ...

35 mm² ...

Page 329

Page 331

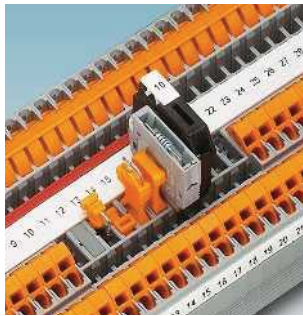
Page 335



Disconnect terminal blocks

6 mm² ...

Page 333



Isolating plugs and component connectors

P...

Page 350



Marker carriers/warning labels

STP ...

Page 352

For end clamps and DIN rails, see Catalog 5

UK... universal terminal blocks



Page 357



Feed-through terminal blocks and ground

terminals

UK ..., USLKG ...

Page 360



Screw cap fuse terminal blocks

UK ...-DREHSI

Page 398



Fuse terminal blocks for NEOZED® and

DIAZED® fuse-links

USEN ...

Page 408



Basic terminal block for isolating plugs and

component connectors

UK ...-TG

Page 410



Fuse and isolating plugs and component

connectors

ST-BE, BES 6

Page 412



Test disconnect terminal blocks

URTK/SP

Page 429



Double-level diode terminal blocks

UKK ...-DIO

Page 432



Thermoelectric voltage terminal blocks

MTKD ...

Page 436



Ground disconnect terminal blocks

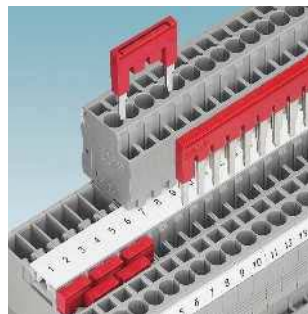
GTF 76

Page 437

Accessories

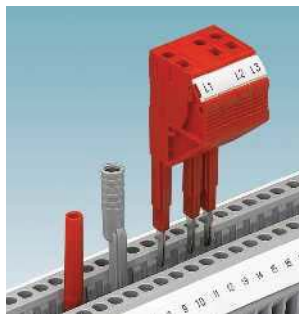


Page 337



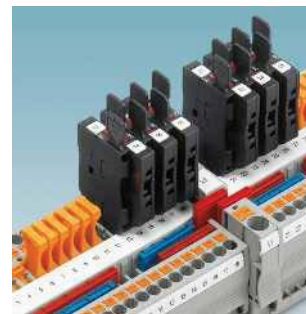
Jumpers
FBS ...
FBSR ...

Page 340
Page 342



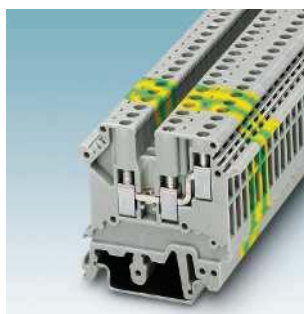
Test accessories
PS ..., MPS ..., PAI ...

Page 346



Fuse plugs
P-FU...-5

Page 349



Three- and four-conductor terminal blocks
UK ...-TWIN
UDK ...

Page 368
Page 372



Double-level terminal blocks
UKK ...

Page 374



Initiator/actuator terminal blocks
DIK ..., DOK ..., VIOK ...

Page 382



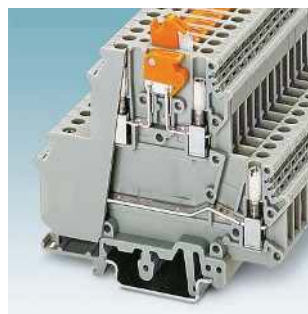
Lever-type fuse terminal blocks
UK 5-HESI N

Page 392



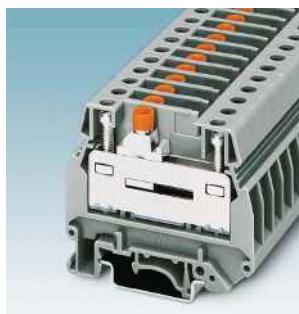
Knife disconnect terminal blocks
MTK ...
UK ...MTK

Page 416
Page 417



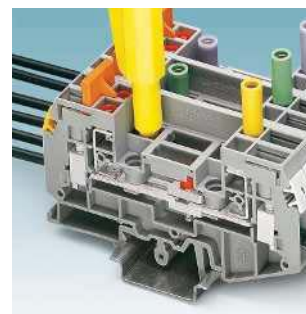
Double-level knife disconnect terminal blocks
UKK ...MTK

Page 418



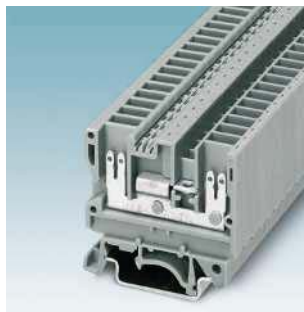
Cross connection terminal blocks
UGSK/S

Page 421



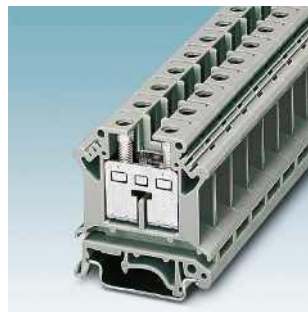
Common mode and cross connection terminal blocks
URTK 6

Page 427



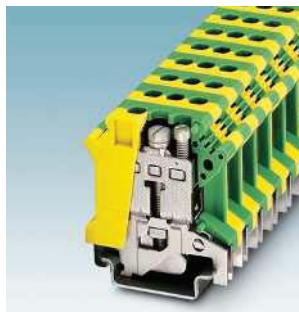
Terminal blocks with spade connection
UVKB 4-FS/FS ...

Page 438



Installation terminal blocks
UIK ...

Page 444



Installation ground terminals
UISLKG ...

Page 446



Neutral disconnect terminal blocks
UKN ...

Page 447

Product range in pictures

From here, you can access the desired product directly



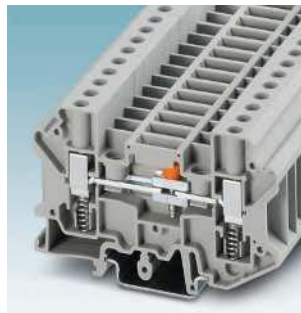
Ceramic terminal blocks
SSK ...

Page 450



Spring-assisted screw terminal blocks
USST ...

Page 454



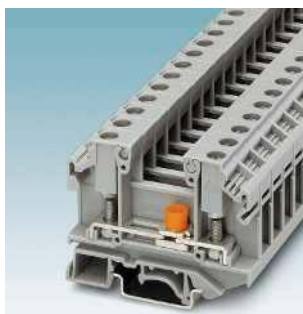
Spring-assisted disconnect terminal blocks
USST-T ...

Page 458



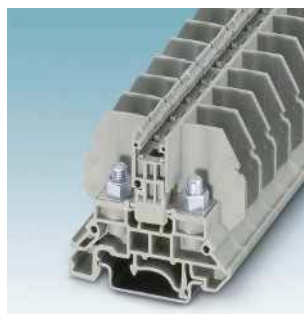
Micro/mini terminal blocks
MT 1,5 ...

Page 462



Bolt connection terminal block with
disconnect function
OTTA 6-T

Page 476



Bolt connection terminal blocks for DIN rail
and direct mounting
RBO ...

Page 478



Bolt connection terminal blocks with
covering hood
RBO ...-HC

Page 484



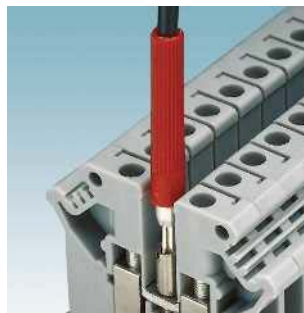
Bolt connection terminal blocks for DIN rail
and direct mounting
RSC ...

Page 486

Accessories



Potential distributors
See Catalog 7, page 618



Test plugs for UK series
PS ...

Page 504



Test plugs for UK series
MPS ...
PS-UK ...

Page 509

Page 509



Warning labels
WS ...

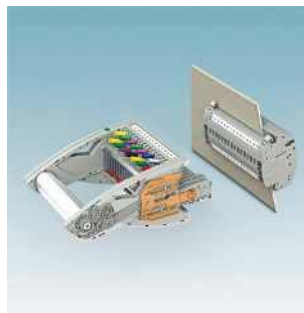
Page 511

Sector-specific solutions



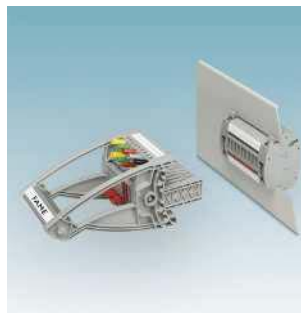
Supports for direct mounting
AB ...

Page 521



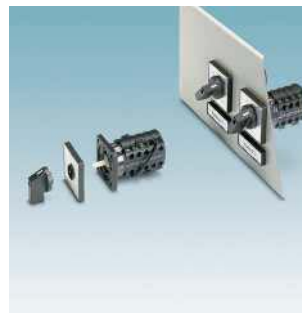
FAME 2 plug-in test system without
operating plug

Page 528



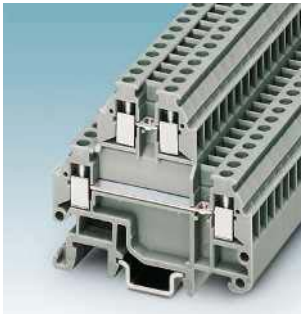
FAME 1 plug-in test system with operating
plug

Page 560



Rotary switches
RS20-US ...

Page 569



Micro/mini terminal blocks
MTTB 1,5 ...

Page 465



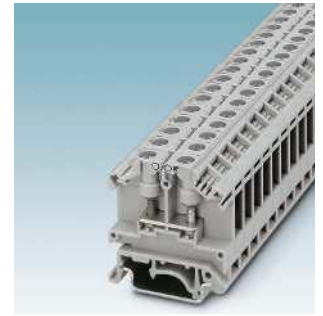
Mini strip terminal blocks
MBK ...

Page 468



Double-level mini terminal blocks
MBKKB ...

Page 470



Bolt connection terminal blocks for DIN rail
and direct mounting
OTTA ...

Page 473



High-current connectors
HV M ...

Page 491



High-current connectors
UHV ...

Page 494



Device terminal blocks
G ..., GE ...

Page 498



Trunk line branch terminals
UDB 2X...

Page 502

SK... shield terminals



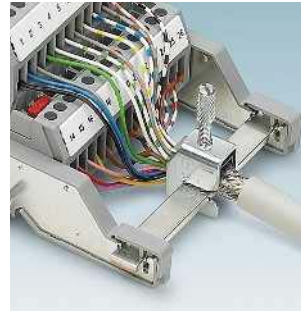
Shield terminals
SK ...

Page 512



Shield terminals
SKS ...

Page 515



Shielded supports for neutral busbars
AB-SK ..., AB/SS ...

Page 516



Double supports
AB-SK 65-D ...

Page 518

Services: terminal strips, CLIPSAFE stainless steel Ex terminal boxes, and empty housings



Service

Page 589



Terminal strips

Page 590



CLIPSAFE stainless steel Ex terminal boxes
and empty housings

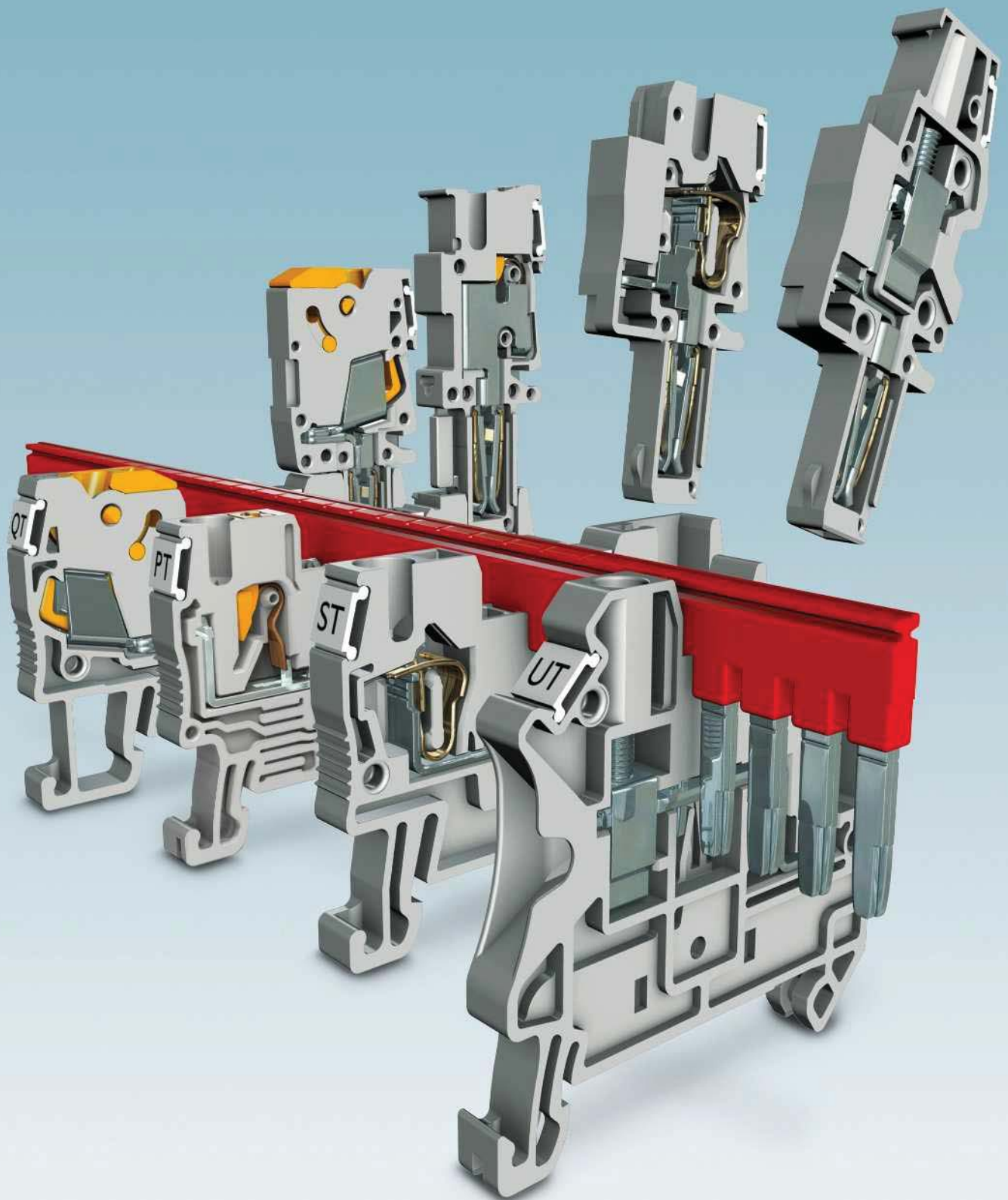
Page 592

Planning and marking software



Planning and marking software
CLIP PROJECT

Page 594



CLIPLINE complete system features

With CLIPLINE complete, the unique terminal block system from Phoenix Contact, the choice of connection technology is yours. The following connection methods are available:

- Universal UT... screw connection
- Simple PT... push-in connection
- Compact ST... spring-cage connection
- Fast QT QUICKON connection
- COMBI plug-in connection solutions
- Robust RT bolt connection

Irrespective of which connection technology you choose, they can all be freely combined, with the same accessories, thanks to the double function shaft.

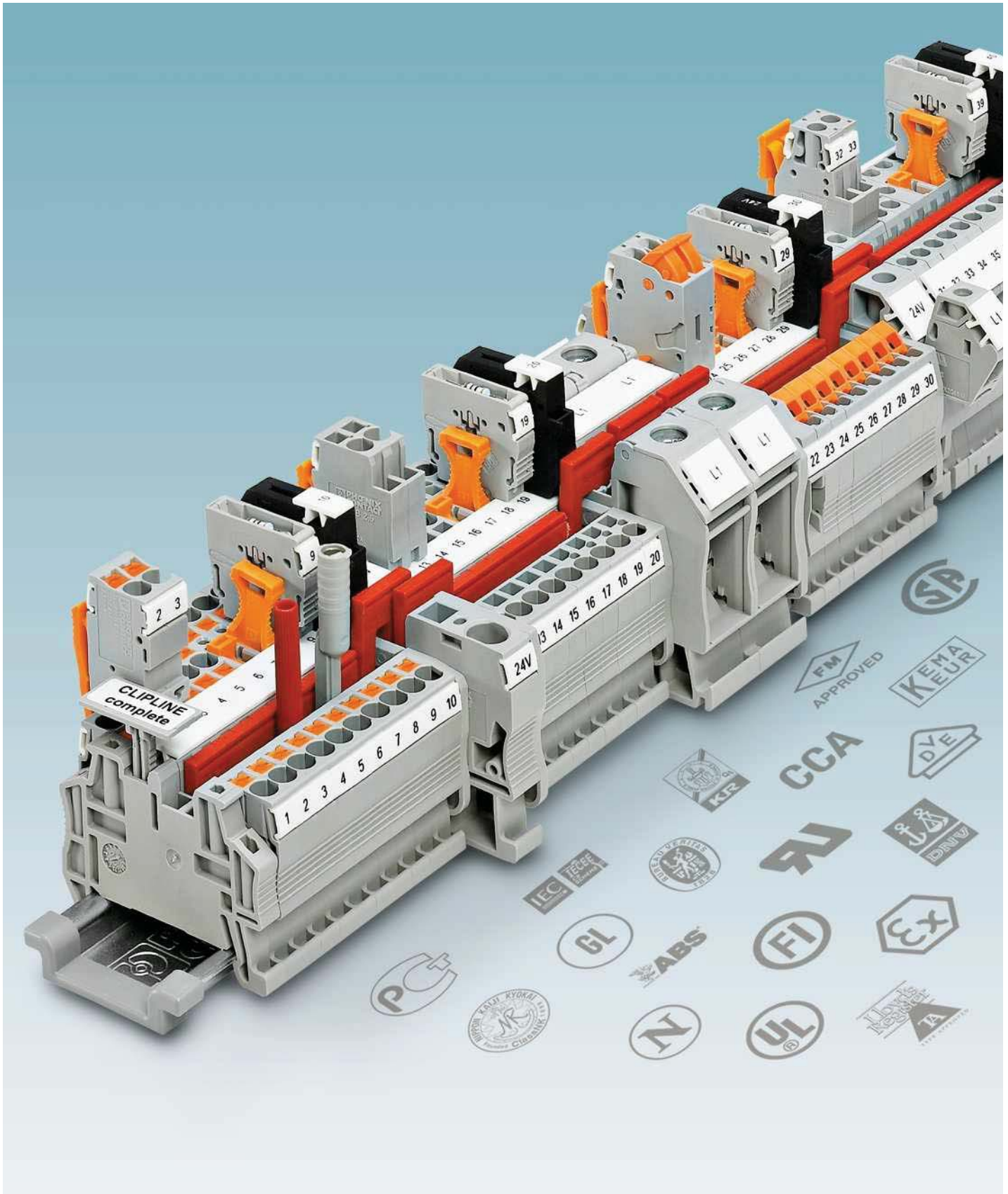
In addition to the flexibility of this terminal block system, CLIPLINE complete also provides added value. The bridging, marking, and test accessories are standardized and can reduce your logistics and storage costs.

The CLIPLINE complete terminal block system has been tested and approved for a wide range of national and international approvals. The maximum level of safety in these standards is achieved by routine testing of the standard CLIPLINE complete terminal blocks according to the ATEX Directive. They can also be used in the Ex e area.

Product range overview	
System features	16

CLIPLINE complete

All connection technologies, one system



General

The CLIPLINE complete system offers you a uniform range of accessories for all connection technologies. Marking and test accessories are standardized and reduce logistics costs. In addition, all terminal blocks of the CLIPLINE complete system can be freely combined with each other using the double function shaft. The standardized plug-in zone of the COMBI basic terminal blocks also allows the connection of modules via individually configurable plugs, regardless of the connection technology.

CLIPLINE complete terminal blocks with screw, spring-cage, push-in, bolt, and plug-in connections enable you to react flexibly to the demands of your customers anywhere in the world.

Flexible jumper system

The same jumper for all connection technologies. To allow fast and individual potential distribution, the terminal blocks in the CLIPLINE complete system have two function shafts. These are arranged in one line over all the terminal blocks, allowing for a combination of connection technologies. The 2- to 50-pos. jumpers make it possible to implement all the tasks of potential bridging within a very short time. Reducing bridges connect, for example, UT... screw terminal blocks and ST... spring-cage terminal blocks.

The plug-in switching jumpers make contact by being securely latched into the function shaft. They create a removable connection between neighboring terminal blocks.

Plug-in connection solutions

The COMBI connection system enables the time-saving and modular configuration of your application. Like the terminal blocks, the COMBI connectors are available with screw, spring-cage, push-in, and fast connection technologies.

The nominal data of up to 41 A and 1000 V has made a connection system for signal and power wiring possible. The system meets the most stringent of vibration requirements. Both the terminal blocks and the plugs are touch proof.

Extensive accessories are available, from latching mechanisms to shield connections.

Multifunctional disconnect zone

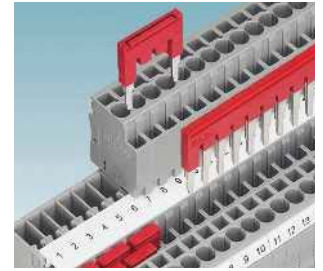
All disconnect terminal blocks in the CLIPLINE complete system have a standardized disconnect zone. Various function plugs are available for use in the disconnect terminal blocks. Isolating plugs are used for simple disconnection. The fuse plugs are designed for the use of cartridge fuse-links. The patented component connector allows you to mount components quickly, without the risk of polarity reversal, and without the need for soldering.

Large-surface marking

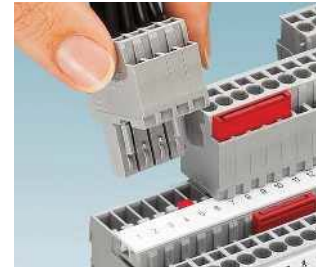
All the terminal points of the terminal blocks in the CLIPLINE complete system have large-surface marking options. This is a precondition for clear wiring and startup and simplifies assignment during testing and maintenance work. Optional large-surface snap-on marker carriers are available for group and terminal strip marking.

Standardized test system

A comprehensive range of test accessories is available in the CLIPLINE complete system. All test plugs make contact in the freely accessible function shaft. For individual measuring lines, a 2.3 mm diameter test plug is available. More complex testing tasks can be implemented using alignable test plugs. The corresponding spacers can be used to assemble individual test adapters perfectly suited for use in test laboratories.



Jumpering



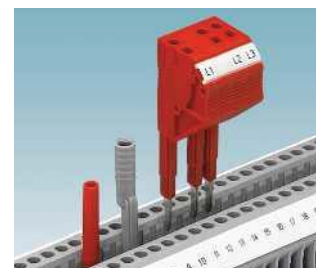
Inserting



Disconnecting

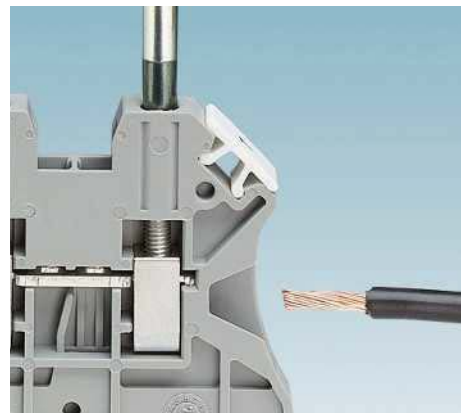
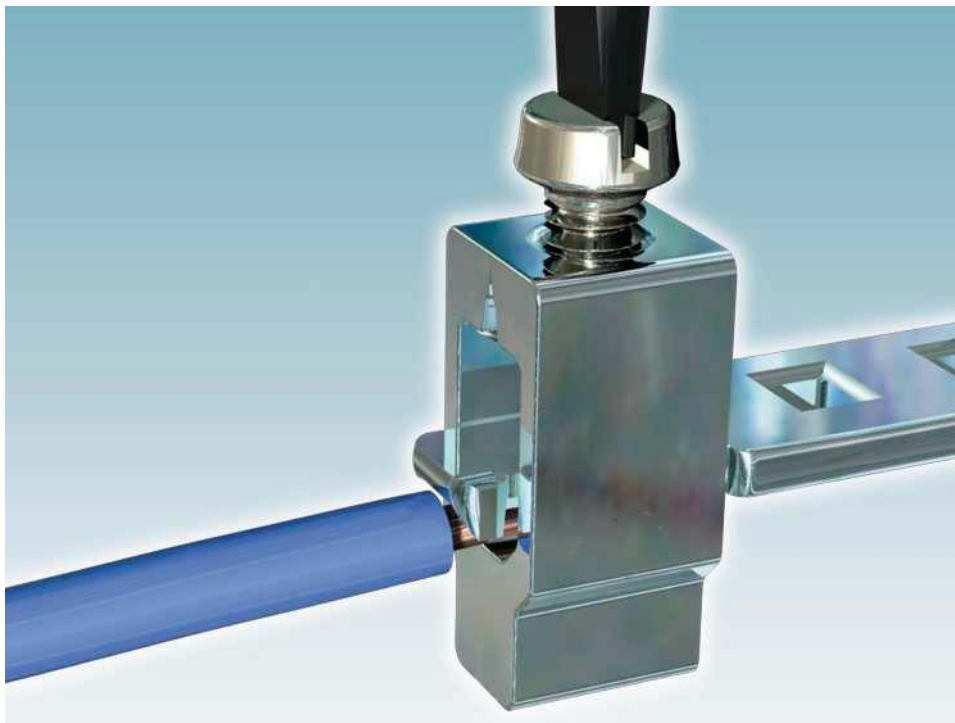


Marking



Testing

System features - screw connection



Material properties

The metal parts of the UT... screw connection terminal blocks are made from high-grade, strain-crack, and corrosion-proof copper alloys as a standard feature. This eliminates the possibility of electrolytic corrosion in the presence of moisture and the risk of rusting. The consequences, such as unreliable electrical contacts and/or jammed screws, are also prevented. Another advantage is the low temperature rise due to good electrical conductivity. The surface of the metal parts is protected by lead-free, galvanic nickel or tin plating.

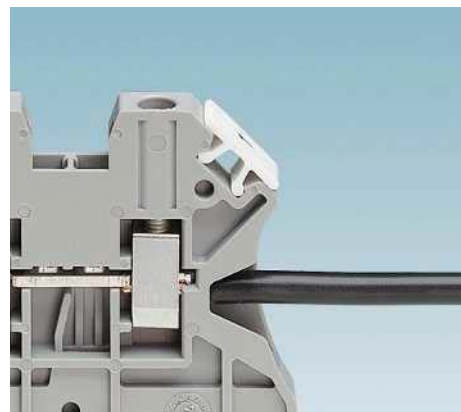
The insulating housing of the UT... screw connection terminal blocks is made from recyclable PA 6.6. This elastic plastic with high impact strength is halogen-free and UV resistant. Further characteristics include the good tropical and termite resistance, high chemical resistance, and excellent aging characteristics. Polyamide 6.6 can be used with operating temperatures up to 130°C and is certified for inflammability class V0 according to UL 94.

Connection principle

UT... screw connection terminal blocks are designed for the most stringent requirements. For more than 80 years, they have proven themselves a billion times over in all applications. An important characteristic is the maintenance-free conductor connection. There is no need to tighten the terminal block screws. The screws are prevented from loosening by the Reakdyn principle, a screw locking technique developed by Phoenix Contact.

Phoenix Contact UT... screw connection terminal blocks can be clamped without any pretreatment. Splicing protection can also be implemented in the form of ferrules. A special characteristic of the screw clamping body is the multi-conductor connection, which is often required.

Very large conductor cross sections up to 240 mm² can also be wired gas-tight and with long-term stability thanks to the high contact forces.



System features - push-in connection



Material properties

All metal parts of the push-in terminal blocks are made from corrosion-free materials. The conductive metals consist of high-grade copper alloys. A particular advantage is the low temperature rise due to good electrical conductivity. The surface of the metal parts is protected by lead-free, galvanic nickel or tin plating.

The contact force for the push-in connection is applied by a leg spring made of high-strength chromium-nickel spring steel.

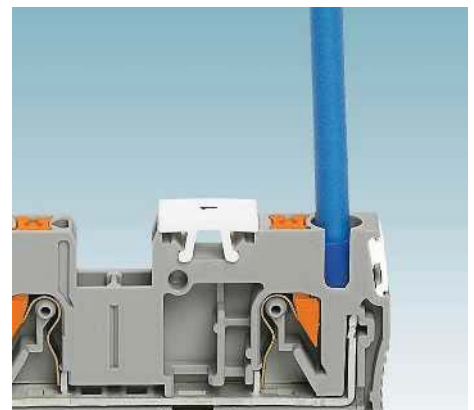
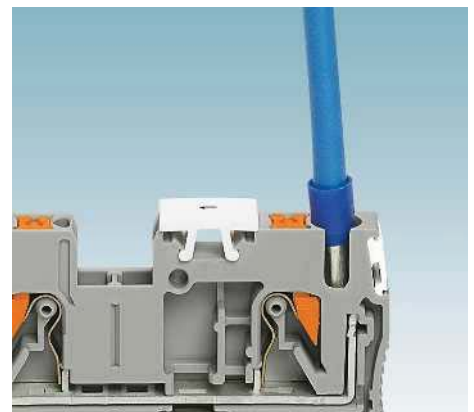
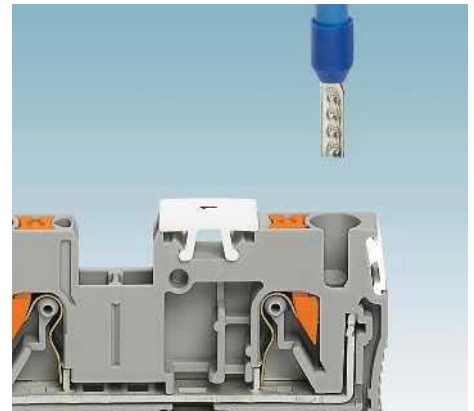
The insulating housing of the terminal blocks is made from recyclable PA 6.6. This elastic plastic with high impact strength is halogen-free and UV resistant. Further characteristics include the good tropical and termite resistance, high chemical resistance, and excellent aging characteristics. Polyamide 6.6 can be used with operating temperatures up to 130°C and is certified for inflammability class V0 according to UL 94.

Connection principle

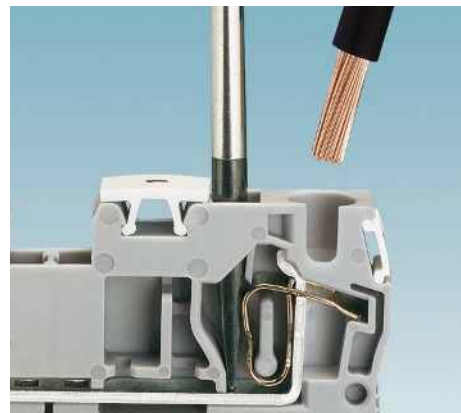
PT... push-in connection terminal blocks have been developed for direct conductor connection. This means that solid conductors or conductors with ferrules can be inserted directly into the terminal block without tools.

The special spring profile enables the easy insertion of conductors with ferrules from 0.34 mm² to 95 mm². The contact spring is opened automatically when the conductor is pushed in and thereby provides the required pressure force against the current bar. Both for releasing conductors and connecting small cross sections from 0.14 mm², the spring is opened by means of the actuation lever – easily and without direct contact with live parts. The actuation lever can be operated with all standard screwdrivers.

The PT... connection technology has been tested and approved for a wide range of approvals. These include, for example, vibration resistance according to railway standard EN 50155 and shock and corrosion resistance according to current shipbuilding registers. It is also certified for process engineering in areas with increased safety (Ex e).



System features - spring-cage connection



Material properties

All metal parts of the spring-cage terminal blocks are made from corrosion-free materials. The conductive metals consist of high-grade copper alloys. A particular advantage is the low temperature rise due to good electrical conductivity. The surface of the metal parts is protected by lead-free, galvanic nickel or tin plating.

The contact force for the spring-cage connection is applied by a spring element made from high-strength chromium-nickel spring steel.

The insulating housing of the spring-cage terminal blocks is made from recyclable PA 6.6. This elastic plastic with high impact strength is halogen-free and UV resistant. Further characteristics include the good tropical and termite resistance, high chemical resistance, and excellent aging characteristics. Polyamide 6.6 can be used with operating temperatures up to 130°C and is certified for inflammability class V0 according to UL 94.

Connection principle

ST... spring-cage terminal blocks have been developed for universal spring-loaded conductor contacting.

The contact force is independent of the user and creates a vibration-proof, gas-tight connection with long-term stability.

The terminal point is opened with a standard screwdriver. After the conductor has been inserted into the clamping space, the screwdriver is removed and the conductor automatically makes contact. The easy operation is a result of the front connection, i.e., the conductor and screwdriver come in parallel from the same direction.

All kinds of copper conductors up to 35 mm² can be clamped without any pretreatment. Splicing protection can also be implemented in the form of ferrules.

Phoenix Contact spring-cage terminal blocks offer a large insertion space, i.e., conductors with ferrules and insulating collars and with a nominal cross section can also be wired.



System features - fast connection



Material properties

The patented contact metals of the QT... fast connection terminal blocks are made from a special, high-grade copper alloy. This combines good electrical conductivity with excellent elastic characteristics.

The surface of the metal parts is protected by lead-free, galvanic nickel or tin plating.

The insulating housing of the fast connection terminal blocks is made from recyclable PA 6.6. This elastic plastic with high impact strength is halogen-free and UV resistant. Further characteristics include the good tropical and termite resistance, high chemical resistance, and excellent aging characteristics. Polyamide 6.6 can be used with operating temperatures up to 130°C and is certified for inflammability class V0 according to UL 94.

Connection principle

QT QUICKON terminal blocks are designed for fast conductor connection. There is no need to strip or implement splicing protection; the cables simply need to be cut to length for contact to be made in a matter of seconds.

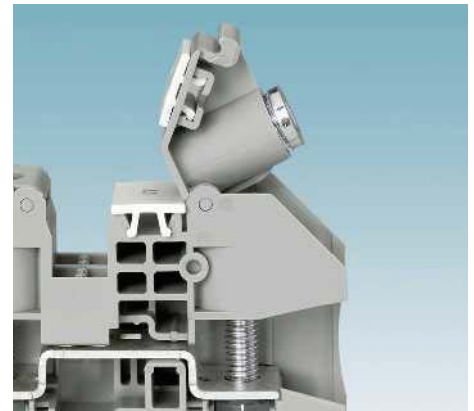
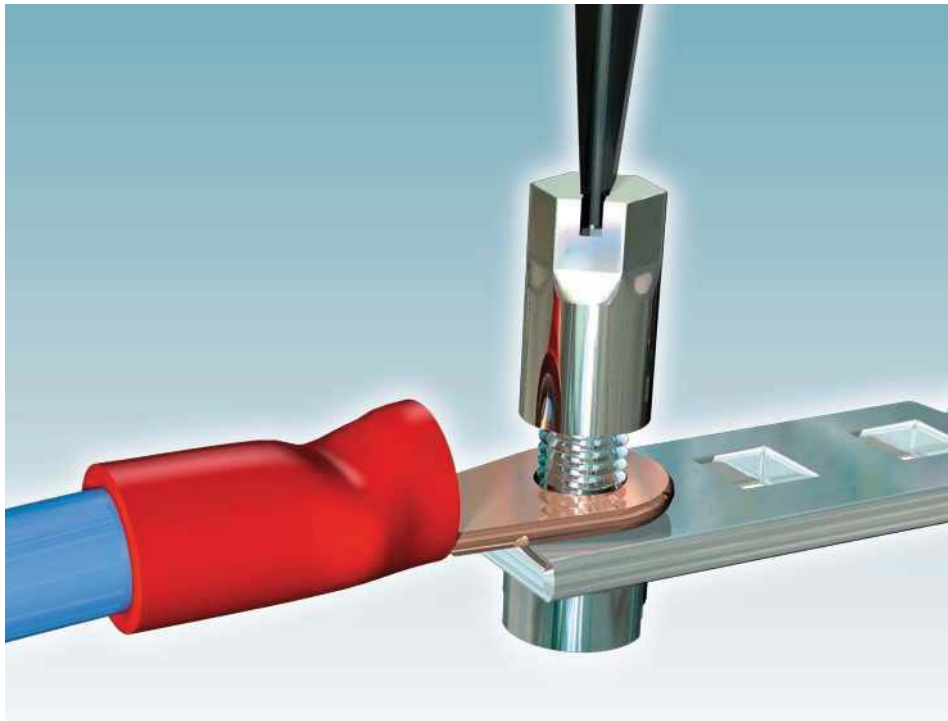
An important characteristic is the space-saving twist connection. Due to the simplicity of the connection, the wiring time is reduced by up to 60 percent. A standard screwdriver is used to operate the terminal blocks and the switching states are clearly signaled by engagement points in the start and end position.

Solid and stranded conductors from 0.25 to 2.5 mm² can be wired without aids such as guide ferrules. When a conductor is connected, the conductor insulation is cut open, displaced, and the conductor is securely engaged in the end position where it makes extensive, gas-tight contact.

The high quality of the QUICKON fast connection is verified by the fact that this connection is certified according to the standard for Ex e applications, as are the screw and spring connections.



System features - bolt connection



Material properties

All metal parts of the bolt connection terminal blocks are made from corrosion-free materials. The conductive metals consist of high-grade copper alloys. Due to their good electrical conductivity, they ensure a low temperature rise. The surface of the metal parts is protected by lead-free, galvanic nickel or tin plating.

The insulating housing of the bolt connection terminal blocks is made from recyclable PA 6.6. This elastic plastic with high impact strength is halogen-free and UV resistant. Further characteristics include the good tropical and termite resistance, high chemical resistance, and excellent aging characteristics.

Polyamide 6.6 can be used with operating temperatures up to 130°C and is certified for inflammability class V0 according to UL 94.

Connection principle

RT... bolt connection terminal blocks have been developed with a robust design and offer convenient wiring for ring cable lugs.

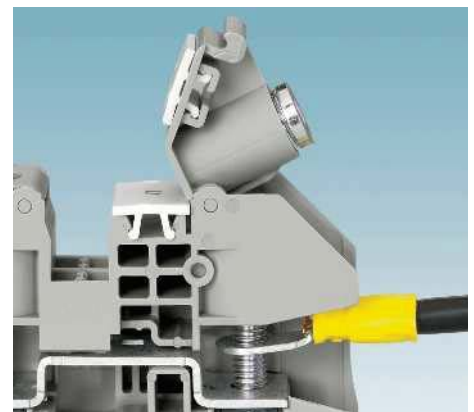
An important characteristic is the hinged cover which can be swung up and which features a captive cap nut. This ensures quick and easy ring cable lug wiring.

The integrated screw locking in the form of a spring retainer guarantees safe use, even in applications which are subject to shock and vibration.

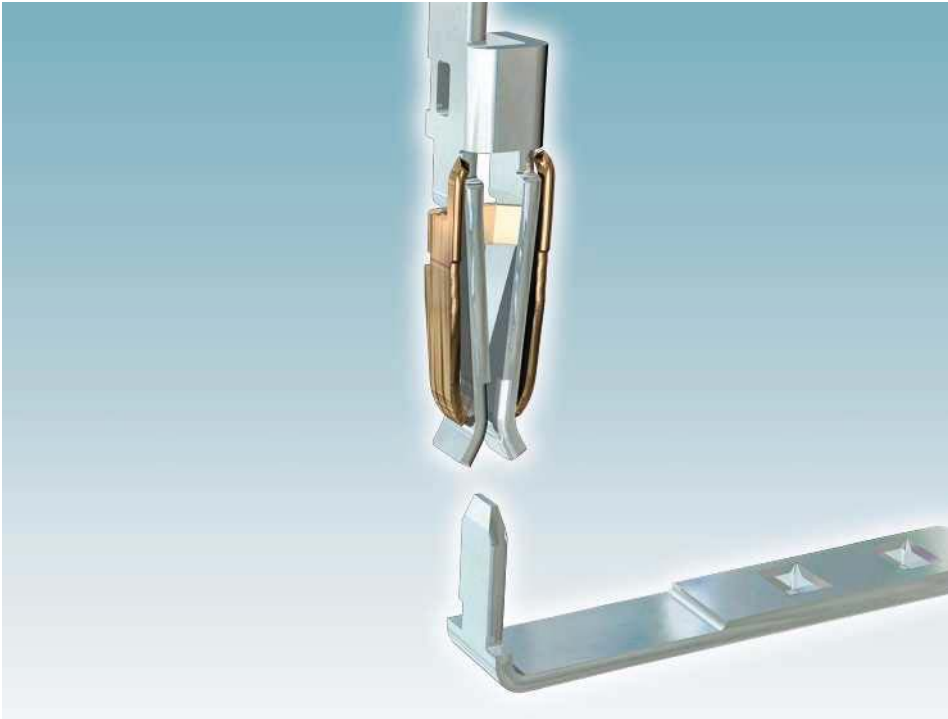
All ring cable lugs which comply with DIN 46234, DIN 46235 or DIN 46237 can be connected.

A special characteristic of the bolt connection is the often required multi-conductor connection, on which up to four cable lugs can be connected per bolt.

All kinds of conductors up to 240 mm² can be wired securely and with long-term stability.



System features - plug-in connection



Material properties

All metal parts of the COMBI connectors are made from corrosion-free materials. The distinction between the electrical and mechanical functions is a particular advantage. The conductive metals consist of high-grade copper alloys. The surface of the metal parts is protected by lead-free, galvanic nickel or tin plating. The high current carrying capacity of the contact is achieved by an integrated covering spring made of chromium-nickel spring steel.

The insulating housing of the COMBI connectors is made from recyclable PA 6.6. This elastic plastic with high impact strength is halogen-free and UV resistant. Further characteristics include the good tropical and termite resistance, high chemical resistance, and excellent aging characteristics.

Polyamide 6.6 can be used with operating temperatures up to 130°C and is certified for inflammability class V0 according to UL 94.

Connection principle

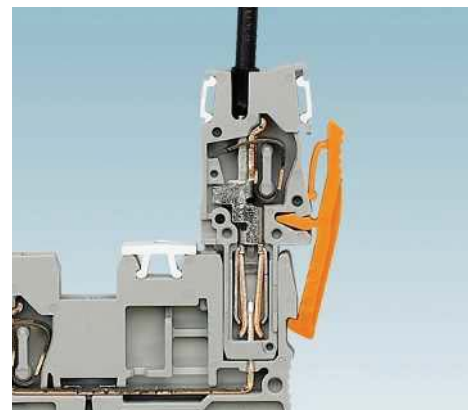
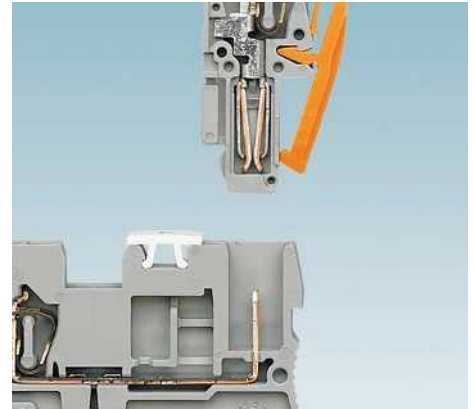
COMBI plug-in connections are designed for the most stringent universal demands in terms of plug-in capability. Here the nominal current of the connected conductor can be carried through the plug-in contact.

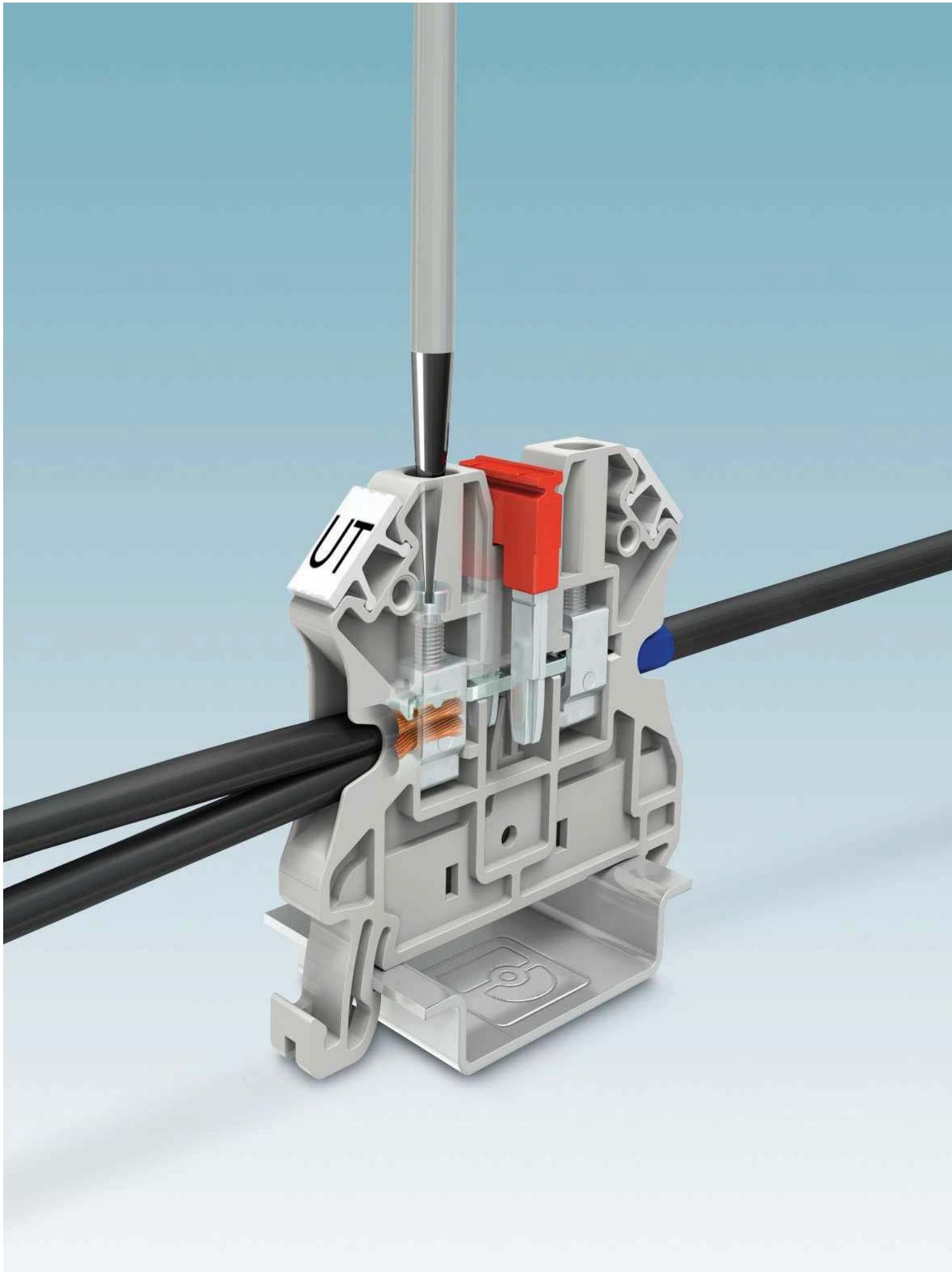
The uniform plug-in zone is an important characteristic. Connectors and basic terminal blocks with four connection technologies can be freely combined with each other, thanks to the uniform plug-in zone.

The modular structure also enables individual self-assembly of the plugs and the couplings.

All kinds of copper conductors can be connected without any pretreatment. Splicing protection can also be implemented in the form of ferrules.

COMBI connectors with all connection technologies offer a large insertion space, i.e., conductors with ferrules and insulating collars and with a nominal cross section can also be wired.





UT... screw connection terminal blocks

The UT... screw connection terminal blocks from the CLIPLINE complete system satisfy the most stringent requirements and cover a wide area of application. They impress with their maintenance-free conductor connection and offer maximum flexibility with their multi-conductor connection. You can connect conductors with a nominal cross section either with or without ferrules. It is not necessary to tighten the terminal block screws, since they are prevented from loosening by the Reakdyn principle, a screw locking technique developed by Phoenix Contact. Very large conductor cross sections up to 240 mm² can also be wired gas-tight and with long-term stability thanks to the high contact forces.

Product range overview

2.5 mm²

Feed-through, multi-conductor, and multi-level terminal blocks and ground terminals	31
Disconnect and knife disconnect terminal blocks	33
Diode and LED terminal blocks	35
Installation terminal blocks	36
Mini feed-through terminal blocks and ground terminals	39

4 mm²

Feed-through, multi-conductor, and multi-level terminal blocks and ground terminals	41
Fuse terminal blocks and lever-type disconnect terminal blocks of the same shape	43
Disconnect and knife disconnect terminal blocks	45
Test disconnect terminal blocks	49
Diode terminal blocks	50
Installation terminal blocks	51
Mini feed-through terminal blocks and ground terminals	51

6 mm²

Feed-through terminal blocks and ground terminals	53
Fuse terminal blocks	53
Disconnect and knife disconnect terminal blocks	54
Test disconnect terminal blocks	56
Installation terminal blocks	58

10 mm²

Feed-through terminal blocks and ground terminals	61
Installation terminal blocks	61

16 mm²

Feed-through terminal blocks and ground terminals	63
Installation terminal blocks	63

35 mm²

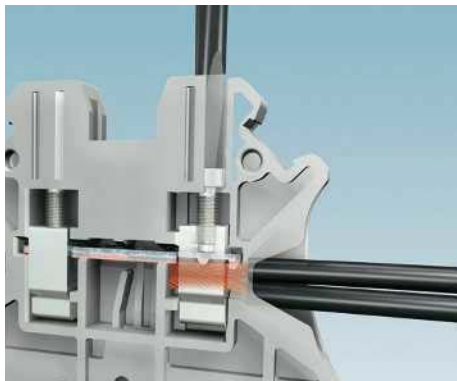
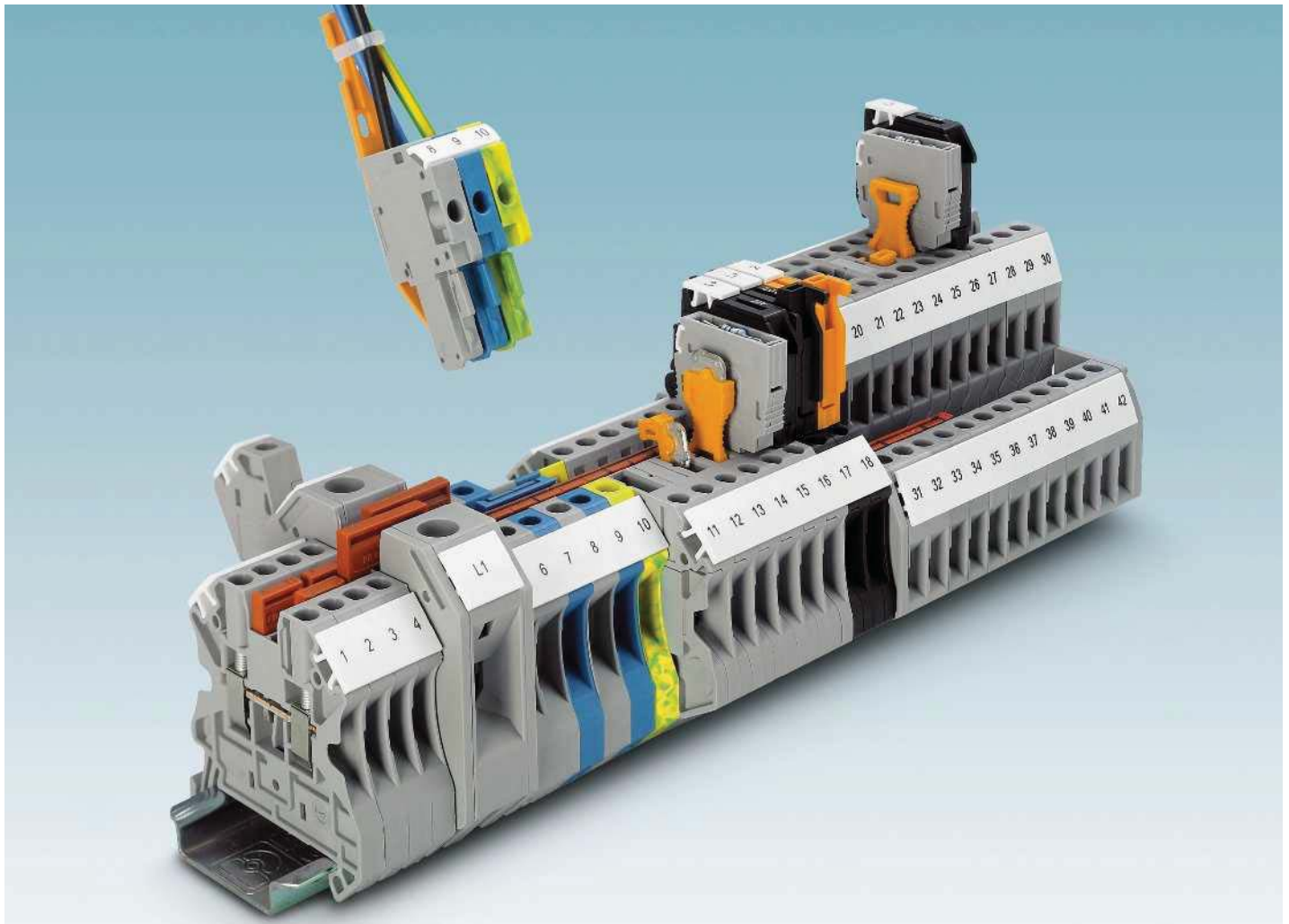
Feed-through terminal blocks and ground terminals	65
Installation terminal blocks	65

50 mm² - 240 mm²

High-current terminal blocks	67
------------------------------	----

Terminal blocks - CLIPLINE complete

UT... screw connection terminal blocks



Universal and zero-maintenance

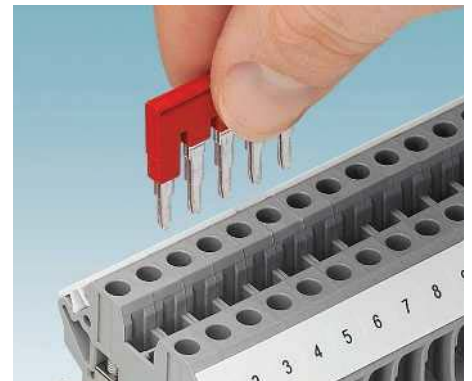
The screw connection is characterized by three main features.

- Global standard
- Multiple conductor connection
- Zero maintenance thanks to Reakdyn principle.



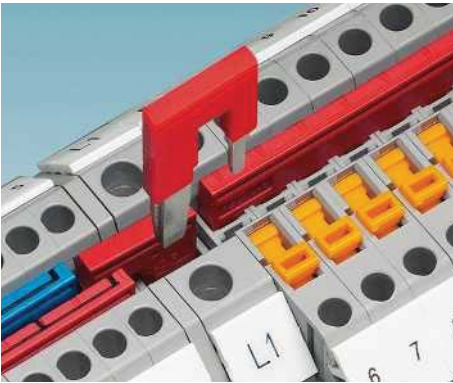
Snap-on PE foot

Ground terminals of the same shape are simply snapped onto the DIN rail in order to make contact. This mechanically and electrically efficient contacting meets all the requirements of the IEC 60947-7-2 standard.

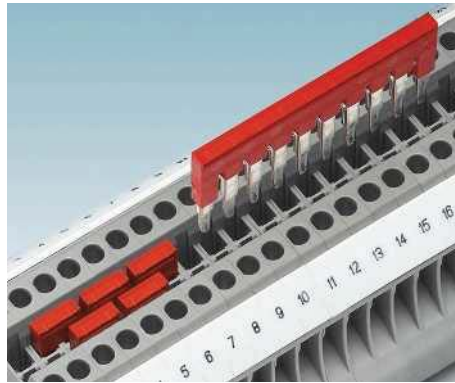


Flexible jumper system

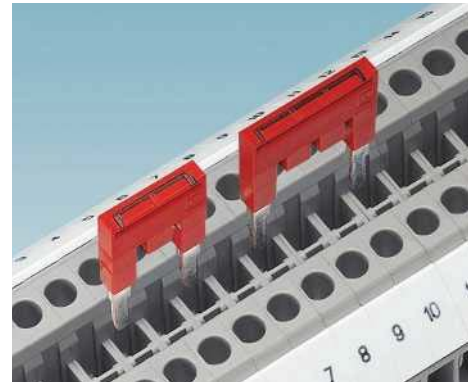
The potential distribution can be implemented at speed with the standardized jumpers. Using two bridge shafts in all terminal blocks makes flexible chain, level or jumping bridges possible.



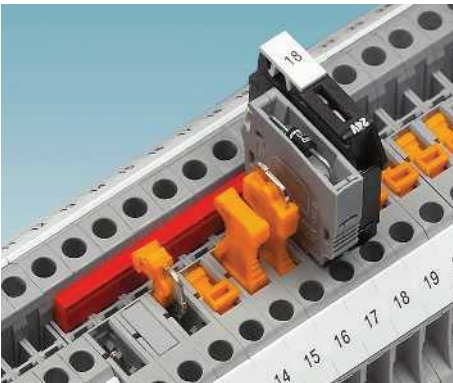
The reducing bridge enables terminal blocks with different nominal cross sections to be connected easily, e.g., a UT 10 terminal block to a UT 2,5. Power blocks can be created quickly using the reducing bridge.



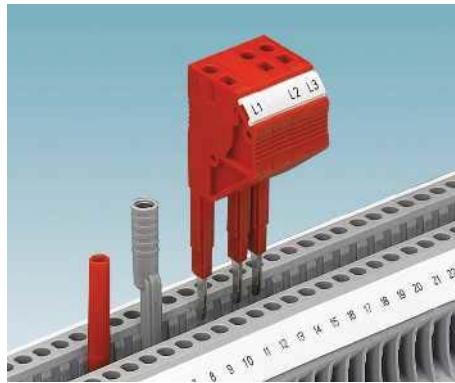
The double function shaft can be used to connect any number of terminal blocks with two-position bridges. The 2 to 50-pos. bridges allow up to 50 terminal blocks to be bridged in one step.



A jumping bridge is created by removing individual contact guides from the standard bridge. Two potentials can then be routed in parallel. The contact points can also be marked.



The P-FIX isolated feed-through connector, P-DI isolating plug, P-CO component connector, and P-FU cartridge fuse plug can be used in the universal plug-in zone of the disconnect terminal block.



A test plug with a 2.3 mm diameter is available for measuring lines. All measurement and test work can be completed at speed using test adapters for 4 mm diameter test plugs and the modular test plugs.



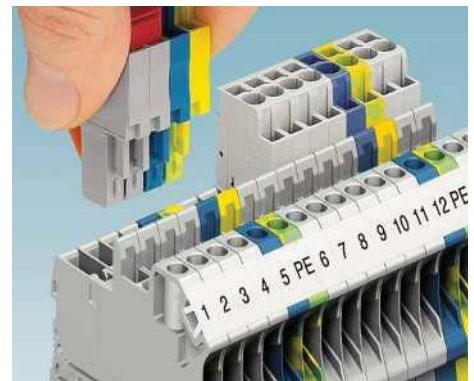
Large-surface and clear marking of the terminal points is essential for reliable and quick installation. Each terminal point in the UT... series can be marked separately.



Disconnect terminal blocks and feed-through terminal blocks UT 4-MTD are available in the same shape as the feed-through terminal blocks. All terminal blocks can be continuously bridged with one another with the double function shaft.



If fully wired, the level offset of the double-level terminal blocks allows the lower connection level to be accessed in full and provides a perfect view of the lower labeling markers and conductor entry funnel.

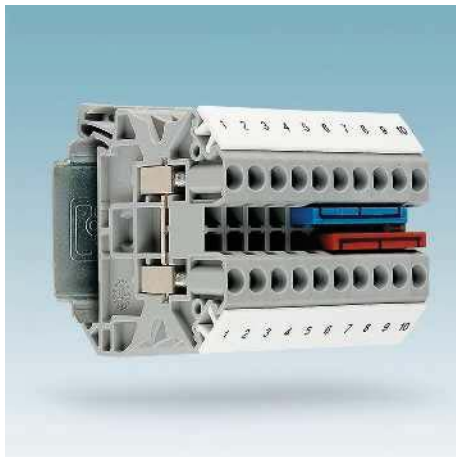


UT-COMBI terminal blocks are available for creating plug-in signal and power wiring. The system is touch proof and offers plugs for self-assembly with extensive accessories. See "COMBI" section, page 225.

Terminal blocks - CLIPLINE complete

UT... screw connection terminal blocks

UT... feed-through, multi-conductor, and multi-level terminal blocks



- Multi-level terminal blocks with PE pick-off and function level
- Signal processing and protection in a confined space, thanks to safety/disconnect lever and universal function zone
- Double bridge shaft enables individual potential distribution and supply
- Suitable for process technology, thanks to Ex nA approval
- Feed-through terminal blocks of the same shape available

i Your web code: **#0056**

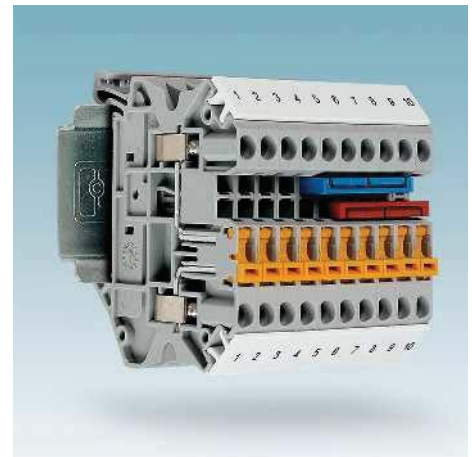
UT... multifunctional terminal blocks



- A wide range of products thanks to versions with PE function or LED display
- Optimum overview of signal connections thanks to a variety of marking options
- Modular expansion up to a maximum of 50 positions, as power terminals are the same shape
- Energy supplied or enhanced by power terminals

i Your web code: **#0075**

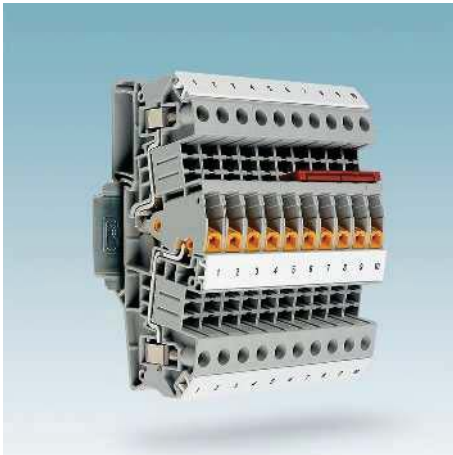
UT... function terminal blocks



- Convenient separation of circuits using lever-type disconnect knife, isolating plug or rotary contact
- User-friendly current measurement thanks to testing facility either side of the disconnect point
- Safe operation as the disconnect lever is locked in the end positions
- Clear identification of the disconnect point thanks to color highlighting
- Individual assembly with disconnect element, fuse plug, component connector, and feed-through connector

i Your web code: **#0057**

UTME... test disconnect terminal blocks



- Easy and safe operation thanks to clear indication of switching states
- Maximum functionality – up to six universal function shafts for potential distribution or for test purposes
- Modular expansion thanks to feed-through terminal blocks and ground terminals of the same shape
- Modular design of transformer circuits thanks to plug-in test disconnect terminal blocks
- Reliable protection of connected current transformers thanks to connector versions with an integrated, leading short-circuit contact

i Your web code: **#0058**

MUT... miniature terminal blocks



- Space saving thanks to compact design and mounting option on a 15 mm DIN rail
- Clear, as all terminal points are marked
- Easy potential distribution thanks to standardized jumpers
- Ideal for installation in small control boxes or terminal boxes, e.g., for motor connection



i Your web code: **#0059**

UTI... installation terminal blocks



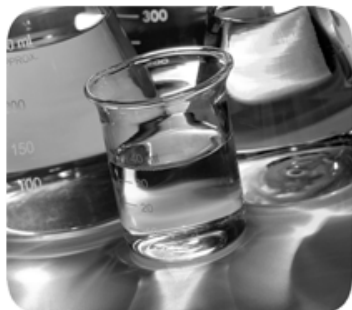
- Space saving thanks to compact three-level distributor terminal blocks of the same shape for single- and multi-phase circuits
- Complete flexibility – all installation terminal blocks with different connection technologies can be combined
- Dielectric test without disconnecting the neutral conductor – thanks to the disconnect slide
- Protection against unintentional actuation since the disconnect slide can be snapped into the limit positions
- Easy terminal block mounting without removing the neutral busbar

i Your web code: **#0060**

	DESIGN, SUPPLY, INSTALLATION, TESTING & COMMISSIONING OF LOCAL SCADA SYSTEM ALONG WITH NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX		
PO: 3761700080	DEWA Doc No.: RFX72-DES-FDS	Contractor Doc No: PRJ212-CMN-INS-FDS-0001	Date: 29-Jul-2018
RFX - 2131600072	FUNCTIONAL DESIGN SPECIFICATION (FDS)		Rev: 1 Attachment-2

ATTACHMENT 2 – FACTORYTALK ASSET CENTRE CONFIGURATION GUIDELINE

FactoryTalk AssetCentre Getting Results Guide



Important user information

Read this document and the documents listed in the additional resources section about installation, configuration, and operation of this equipment before you install, configure, operate, or maintain this product. Users are required to familiarize themselves with installation and wiring instructions in addition to requirements of all applicable codes, laws, and standards.

Activities including installation, adjustments, putting into service, use, assembly, disassembly, and maintenance are required to be carried out by suitably trained personnel in accordance with applicable code of practice. If this equipment is used in a manner not specified by the manufacturer, the protection provided by the equipment may be impaired.

In no event will Rockwell Automation, Inc. be responsible or liable for indirect or consequential damages resulting from the use or application of this equipment.

The examples and diagrams in this manual are included solely for illustrative purposes. Because of the many variables and requirements associated with any particular installation, Rockwell Automation, Inc. cannot assume responsibility or liability for actual use based on the examples and diagrams.

No patent liability is assumed by Rockwell Automation, Inc. with respect to use of information, circuits, equipment, or software described in this manual.

Reproduction of the contents of this manual, in whole or in part, without written permission of Rockwell Automation, Inc., is prohibited.

Throughout this manual, when necessary, we use notes to make you aware of safety considerations.



WARNING: Identifies information about practices or circumstances that can cause an explosion in a hazardous environment, which may lead to personal injury or death, property damage, or economic loss.



ATTENTION: Identifies information about practices or circumstances that can lead to personal injury or death, property damage, or economic loss. Attentions help you identify a hazard, avoid a hazard, and recognize the consequence

Important: Identifies information that is critical for successful application and understanding of the product.

Labels may also be on or inside the equipment to provide specific precautions.



SHOCK HAZARD: Labels may be on or inside the equipment, for example, a drive or motor, to alert people that dangerous voltage may be present.



BURN HAZARD: Labels may be on or inside the equipment, for example, a drive or motor, to alert people that surfaces may reach dangerous temperatures.



ARC FLASH HAZARD: Labels may be on or inside the equipment, for example, a motor control center, to alert people to potential Arc Flash. Arc Flash will cause severe injury or death. Wear proper Personal Protective Equipment (PPE). Follow ALL Regulatory requirements for safe work practices and for Personal Protective Equipment (PPE).

Allen-Bradley, Rockwell Software, Rockwell Automation, and TechConnect are trademarks of Rockwell Automation, Inc.

Trademarks not belonging to Rockwell Automation are property of their respective companies.

	Chapter 1	
Introduce FactoryTalk AssetCentre	Activation	7
	About the documentation set.....	8
	Online help.....	8
	About this book.....	8
	Contact Technical Support	8
	Chapter 2	
Navigate the FactoryTalk AssetCentre client	Run the FactoryTalk AssetCentre client.....	11
	Elements of the FactoryTalk AssetCentre client window	11
	Asset view.....	12
	Asset	12
	Design mode.....	12
	Asset catalog	13
	About asset types	14
	Workspace pane.....	17
	Toolbar.....	18
	Menu bar.....	19
	Right-click menus.....	19
	Status bar.....	19
	Chapter 3	
About FactoryTalk AssetCentre Web Client	Access FactoryTalk AssetCentre Web Client.....	21
	Chapter 4	
Quick Start 1: Configure the system	Quick Start steps for configuring the system.....	23
	Step 1: Add users to the FactoryTalk Directory	24
	Step 2: Add client computers.....	24
	Step 3: Configure security for FactoryTalk AssetCentre.....	25
	Policy settings and their meanings	26
	Step 4: Add contacts to the Address Book	28
	Step 5: Set up FactoryTalk AssetCentre database limitations	29
	Step 6: Configure the SSL protocol.....	30
	Create an SSL certificate	31
	Import the SSL certificate to the Internet Information Services (IIS) Manager.....	31
	Add the certificate authority to client and agent computers.....	32
	Configure a site binding.....	32

Enable secure communication between the server, client(s) and agent(s)	33
Configure SSL settings for FactoryTalk AssetCentre Web Client	34
Step 7: Configure Windows Authentication	36
Turn on Windows Authentication mode in Internet Information Services (IIS)	36

Chapter 5

Quick Start 2: Design the asset tree

Quick Start steps for designing the asset tree	39
Step 1: Plan the organization of your asset tree	39
Step 2: Add assets to the asset tree	41
Use Asset Inventory to add assets to the asset tree	45
Step 3: Change security settings for an asset	48

Chapter 6

Quick Start 3: Set up Disaster Recovery schedules

Quick Start steps for setting up schedules	52
Step 1: Set up Agent Groups and agent computers in them	52
Create an agent group	53
Create an agent computer	53
Step 2: Create a schedule for the desired Disaster Recovery operation	54
Step 3: Set up recipient lists for schedule results	55
Send an End of Schedule report	56
Send an operation-specific report	56
Step 4: Run schedules	57
Run schedules by making them active	57
Run schedules manually	57

Chapter 7

Quick Start 4: View and search logs

Quick Start steps for viewing and searching logs	60
Step 1: View logs	60
Step 2: Create a search	62
Step 3: Set search security	66
Step 4: Run searches	67
Make a search active	67
Run searches manually	67
Step 5: View and print search results	68

Chapter 8

Quick Start 5: Open and edit files in Archive

Quick Start steps for managing files in Archive	70
Step 1: Set a working folder	70
Step 2: Check out a file for editing	71

Step 3: Check in a file	73
Step 4: Get a read-only version of a file	74
Step 5: Open a file for viewing	76

Chapter 9

Quick Start 6: Manage Rockwell Automation hardware life cycle

Quick Start steps for managing Rockwell Automation hardware life cycle	79
Step 1: Synchronize life-cycle status	79
Step 2: Refresh life-cycle status	80
Step 3: View detailed life-cycle status	81

Chapter 10

Troubleshoot

Troubleshoot the FactoryTalk AssetCentre client	83
If the client fails to start	83
If the client cannot communicate with the server	84
If you cannot enter Design Mode	85
If you cannot connect to PanelView Plus devices	85
If you cannot connect to MobileView devices	85
Troubleshoot Schedules	86
If a schedule did not run	86
If a schedule no longer appears on the Schedules tab	86
If an asset is missing from a schedule	86
My schedule contains extra devices that I don't want in the schedule	87
If you are prompted to install agents when creating a Disaster Recovery schedule	88
If you see the message "Failed to create RSLogix 5 [or 500] data [or program ladder] file list"	88
If the scheduled Disaster Recovery operation never completes	89
Troubleshoot e-mail notifications	89
If e-mail notifications do not reach their recipients	89
Troubleshoot Logs	89
If you cannot view a log	90
If no data appears in a log	90
If you cannot refresh a log	90
If you cannot show a previously viewed log	90
Troubleshoot Archive	90
If you cannot check in a file	91
If you cannot open a file	91
If the wrong program opens a file	91
If a button is not available	91
If you performed a recursive check out and the subfolders didn't copy	91
Legal Notices	93

Legal Notices Index

Introduce FactoryTalk AssetCentre

FactoryTalk® AssetCentre monitors your factory automation system, provides centralized tools to minimize downtime due to unauthorized actions or failing devices, and manages the life cycle of Rockwell Automation hardware devices in the system. It does this by:

- securing access to actions within the FactoryTalk AssetCentre system. For information about security, see [Quick Start 1: Configure the system](#) on [page 23](#).
- managing device configuration files. For more information about configuration files, see [Quick Start 2: Design the asset tree](#) on [page 39](#).
- providing a disaster recovery system that verifies your devices' program and configuration files against protected master files, ensuring quick and accurate recovery if a problem should occur. For information about Disaster Recovery, see [Quick Start 3: Set up Disaster Recovery schedules](#) on [page 51](#).
- monitoring FactoryTalk-enabled software products and logging system events and user actions (recorded in the Event log and Audit log respectively). For information about logs, see [Quick Start 4: View and search logs](#) on [page 59](#).
- providing version control and archiving of program files and documents. For information about Archive, see [Quick Start 5: Open and edit files in Archive](#) on [page 69](#).
- synchronizing life-cycle information in the FactoryTalk AssetCentre server and client with the data on the [Rockwell Automation life cycle website](#). For information about life-cycle management, see [Quick Start 6: Manage Rockwell Automation hardware life cycle](#) on [page 79](#).
- managing process device calibration, including scheduling and tracking (Calibration Management capability only). For more information, refer to the *Calibration Management* chapter of the online help.
- managing and configuring DTM devices (Process Device Configuration capability only). For more information, refer to the *Process Device Configuration* chapter of online help.

Activation

FactoryTalk AssetCentre software is activated on two criteria:

- capacity (number of devices)

- capability (purchased functionality)

In addition, the FactoryTalk AssetCentre server must be activated. For more information on activation, refer to the *Activation in FactoryTalk AssetCentre* topic of the online help.

About the documentation set

The documentation set includes:

- **FactoryTalk AssetCentre Installation Guide** (Document ID FTAC-IN005_-EN-E). Use this manual to install the FactoryTalk AssetCentre system.
- **FactoryTalk AssetCentre Getting Results Guide** (Document ID FTAC-GR002_-EN-E, this document). Use this manual to get started using the FactoryTalk AssetCentre system.
- **Online help.** Use the help for assistance while using the FactoryTalk AssetCentre system.
- **Documentation for additional purchased capabilities.** You may have purchased additional FactoryTalk AssetCentre capabilities (such as Disaster Recovery, Calibration Management, or Process Device Configuration). Documentation for those capabilities is included in the online help.

This manual is intended to give a general overview of the software. For more detailed information, please refer to the *FactoryTalk AssetCentre online help*.

Online help

Online help is available from the **Help** menu, by pressing **F1** or clicking the **Show Help** button, or by clicking the **Help** button on any dialog box in the FactoryTalk AssetCentre software.

About this book

This manual provides you with information on how to get started using your FactoryTalk AssetCentre system. It is not intended to be a comprehensive users guide. For complete information on all features, tasks, and interface elements, refer to the online help.

This book is written for FactoryTalk AssetCentre users. We assume you are familiar with:

- Microsoft® Windows® operating systems
- RSLink® communication software
- Rockwell Software® programming tools for programmable logic controllers
- control networks such as DeviceNet and programmable logic controllers such as PLC-5® and ControlLogix processors

Contact Technical Support

If you cannot find answers to your questions in this manual, the online help, or on the Technical Support Web site, call Technical Support.

- **Phone**—440-646-3434 in the USA
- **Technical Support hours of operation**—8:00 AM - 5:00 PM

If you are not located in the USA and want to contact Rockwell Automation Support by telephone, go to <https://www.rockwellautomation.com/global/support/overview.page>, click **Find Local Support**, then click **Phone/Onsite Support**, and then select your country for information about contacting your local support organization.

When you call you should be at your computer and be prepared to give the following information:

- the product version number
- the type of hardware you are using
- the exact wording of any messages that appeared on your screen
- a description of what happened and what you were doing when the problem occurred
- a description of how you tried to solve the problem

Tip: Select **Help > About** from the **Menu** bar to show the product serial number and product version number.

For information about all of the products available from Rockwell Software or for technical support, go to one of the following sites:

- <https://www.rockwellautomation.com/rockwellsoftware/overview.page>
- <https://www.rockwellautomation.com/global/support/overview.page>
- <https://rockwellautomation.custhelp.com>

Navigate the FactoryTalk AssetCentre client

All actions in FactoryTalk AssetCentre take place in the FactoryTalk AssetCentre client. Changes you make in the client window are stored on the FactoryTalk AssetCentre server.

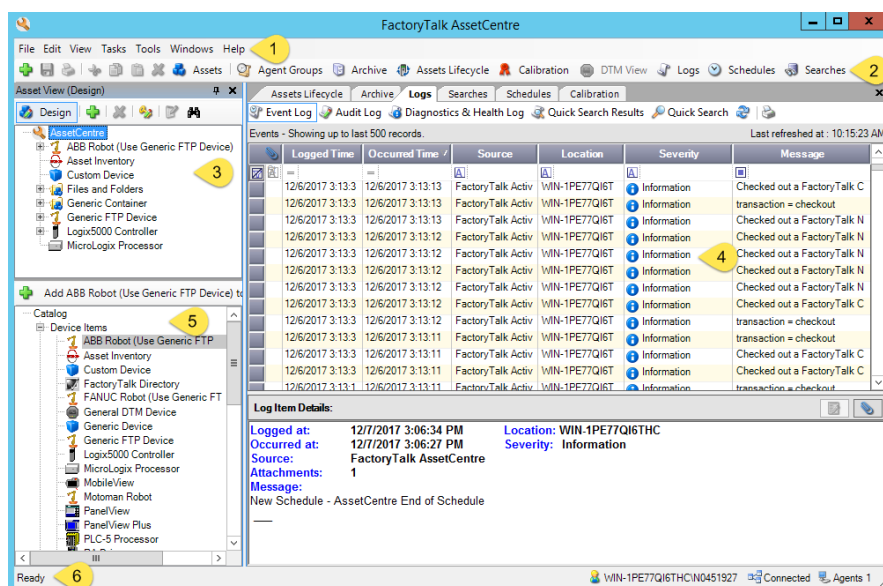
Run the FactoryTalk AssetCentre client

To start the FactoryTalk AssetCentre Client

- Using Windows Search, find **FactoryTalk AssetCentre Client**, and then double-click the name.

If the client fails to start properly, see [If the client fails to start](#) on [page 83](#).

Elements of the FactoryTalk AssetCentre client window



The screen includes the following items:

- Menu bar
- Toolbar
- Asset view

It shows an assets tree that you create to represent your plant.

- Workspace pane

It shows the information and controls of the tools:

- Address Book
- Agent Groups
- Archive
- Assets Lifecycle
- Calibration
- DTM View
- Logs
- Schedules
- Searches

5. Asset catalog

Available in the design mode, it lists all the types of assets that you can add to the assets tree in the asset view.

6. Status bar

It shows the following information:

- The currently logged on user
- The status of the connection to the server
- The number of connected agent computers in the system

Asset view

Everything that you do in FactoryTalk AssetCentre begins with an asset. The Asset View shows the asset tree, a representation of your plant. In the asset tree, you can include all of the assets (anything from a device to a program to a procedure document) that you want to control, back up, or monitor.

Asset

An asset in FactoryTalk AssetCentre represents items of value in your automation system — things you want to control and to which you want to monitor access. Assets can be devices (controllers, drives, or robots), process devices (that control or measure process variables), files (program files or even drawings or word processing files), folders, or containers of other assets. While FactoryTalk AssetCentre is intended to handle files for automation projects, any kind of file can become an asset in FactoryTalk AssetCentre.

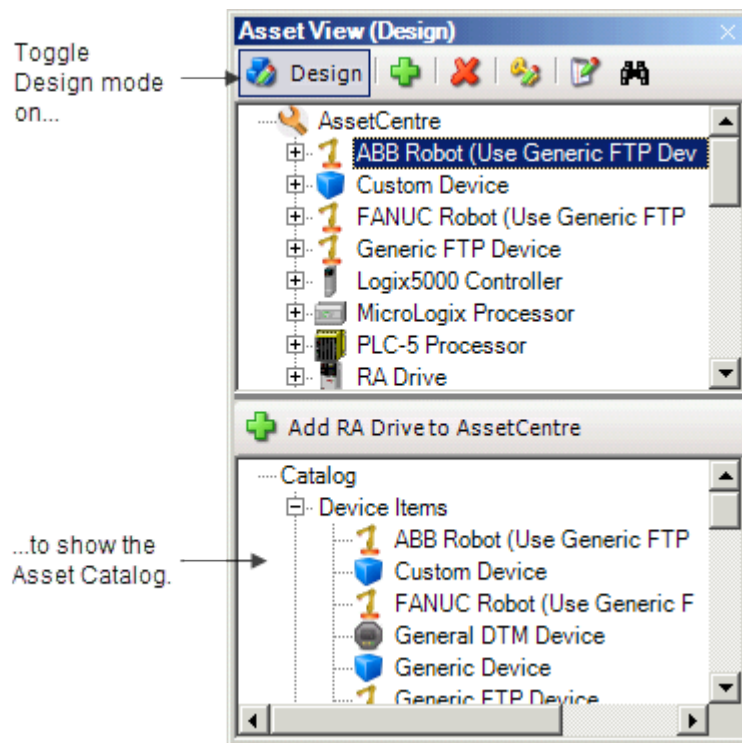
Design mode

In this mode, you can:

- Set up or modify the asset tree in the Asset View so that it represents your system.

- Add devices to the asset tree from the Asset Catalog or edit devices already in the asset tree. The Asset Catalog is only shown in Design mode.
- Set up or modify the agent group tree in the Agent Groups plug-in.

To enter Design mode, click the **Design** button in the Asset View. The **Design** button toggles Design mode on and off. You can also, on the **Menu bar**, select **Edit > Design Mode** or press **F3**. Only one user in your system can be in Design mode at a time.



Tip: You must have **Switch to Design mode** permission to enter Design mode. See [Step 3: Set Feature Security for FactoryTalk AssetCentre](#) on [page 25](#).

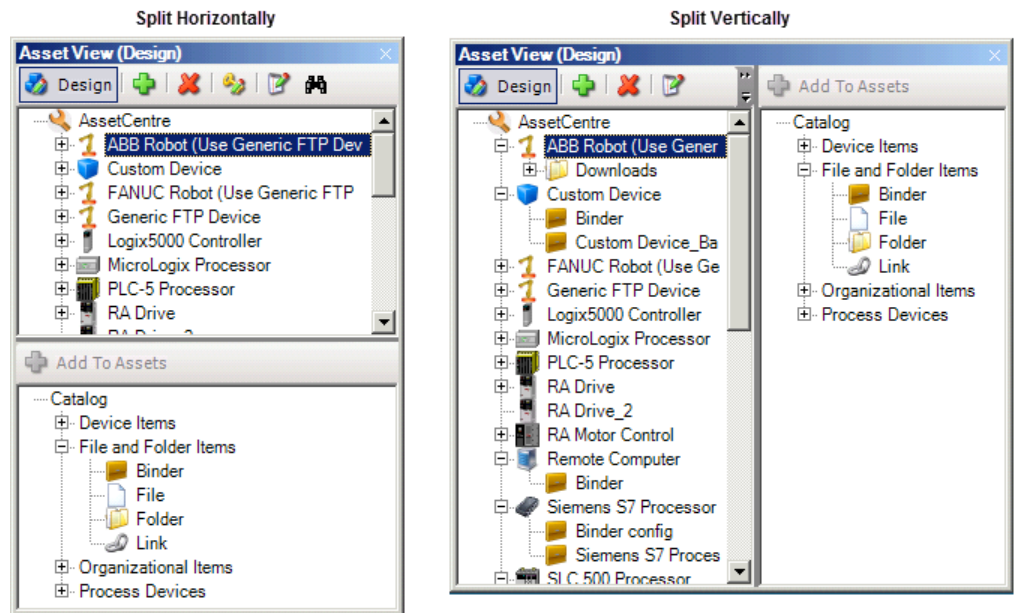
If you have **Switch to Design mode** permission and still cannot enter Design mode to view the Asset Catalog, see [If you can't enter Design Mode](#) on [page 85](#).

Asset catalog

The Asset Catalog lists all the types of assets that can be added to the asset tree. The Asset Catalog is only available when the Asset View is in Design mode. In Design mode, you will use the Asset Catalog to select and add assets by dragging them from the Asset Catalog to the asset tree. For information about adding assets to the asset tree, see [Step 2: Add assets to the asset tree](#) on [page 41](#).

The Asset Catalog can be positioned either below the Asset View or beside the Asset View.

- To position the Asset Catalog below the Asset View, select **View > Layout > Split Horizontally**.
- To position the Asset Catalog beside and to the right of the Asset View, select **View > Layout > Split Vertically**.



About asset types

Assets fall into these categories:

- device items
- files and folders
- organizational assets
- process devices

Device items

Devices can be placed in the asset tree in the root or in a container. Device assets, except for Asset Inventory and Generic Device, count toward capacity activation.

Most device assets are used with the Disaster Recovery capability. A device is a physical automation device. Available device assets are Rockwell Automation controllers; Siemens SIMANTIC S5 and S7 processors; Rockwell Automation PanelView operator interfaces; PanelView Plus operator interfaces; MobileView operator interfaces; FTP Devices, including a variety of robots; Rockwell Automation drives; remote computers; and Custom Devices.

- The **Asset Inventory** asset can be used to scan physical automation devices on the network. When you run a backup or compare schedule on an Asset Inventory asset, the Asset Inventory agent service scans the

connected devices and computers on the network and stores unique identification information about hardware, firmware, and software in the backup data. You can open the backup data in grid view to see the detailed scanning result of devices and associated software. You can also add the scanned assets to the asset tree or update assets in the asset tree with different properties.

- The **FactoryTalk Directory** asset can be used to run a schedule that backs up the FactoryTalk Directory of your system on a regular basis.
- A **Generic Device** is included in the catalog so that you can add unsupported devices to the asset tree. Future versions will support additional device types, such as valves, sensors, pumps, and so on. Future versions will also support compound assets such as a mixing tank with several associated devices: sensors, valves, a pump, a logic controller, and so on.
- The **General DTM Device** asset is for use with the Process Device Configuration capability. Use it to add field devices that have a DTM to the asset tree.
- The **Generic FTP Device** asset is used for devices that use FTP, like robots and drives (instead of a brand-specific robot or drive asset).
- The **Remote Computer** asset can be used with the Disaster Recovery capability to back up and verify the contents of a specified shared folder on a computer in the system. A binder asset is used to specify which files within the shared folder should be operated on. For more information click **Help** on the dialog boxes that are shown when adding a remote computer and binder to the asset tree.

Files and folders

These types of assets can be placed under any device or container in the asset tree.

- A **Binder** is a collection of files and folders that is treated as a unit. For example, when you check out a binder all the contents of the binder are checked out and placed in your working folder.
- A **File** in the asset tree can be any type of data file, from a device's configuration file, to a text file, to a CAD drawing.
- A **Folder** is simply a container in which to place files. You may want to organize files within a folder if you have many files associated with a component or area of your plant, such as a procedure document, an inventory spreadsheet, CAD drawings, and so on. Folders can only contain Files, Binders, and Links, not Devices.
- A **Link** to a binder or file is similar to a shortcut in Microsoft Windows. It is not a second copy of the file or binder, but rather a link to an existing file or binder in the asset tree. Including the same file or binder in several

locations in the asset tree would compromise version control for that file or binder. Instead, place a link to the file or binder in the additional locations.

Organizational assets

An organizational asset can be placed in the root or in another container in the asset tree.

- A **Generic Container** provides a means of representing a functional area of your plant that is comprised of multiple devices. For example, a wash rack might be comprised of a processor, a robot, valves, flow meters, and so on. (Valves and flow meters are not included in FactoryTalk AssetCentre version 7.10.00. Additional device types will be added in future releases. For the time being, they could be represented by a Generic Device.)

Process devices

Process devices can be placed in the asset tree in the root or in a container. Process Device assets count toward capacity activation.

Process Device assets are used with the Calibration Management capability. (The Instrument asset in this category is also used with the Process Device Configuration capability.) Process device assets are used to control or measure process variables such as temperature, level, flow, pressure, or pH. These devices are used to calibrate other process devices, are themselves calibrated, or are used to create logical groupings for calibration procedures.

- **Equipment** assets are not calibrated and are used to group together multiple instruments and loops (which are calibrated) that make up a larger device such as a boiler or extruder. Equipment records may also be used to group together assets that are related, but not necessarily connected, such as a manufacturing line. By grouping all process devices for calibration under an equipment asset, calibration activity for that piece of equipment can easily be organized and managed. They can be placed under system process devices.
- **Instrument** assets are single devices used in the process, control, or laboratory system that require calibration. They are stand-alone components that are building blocks for more complex devices. Examples are meters, calipers, sensors, oscilloscopes, transmitters, and gauges. They can be placed under system, loop, and equipment process devices.

Instrument assets can be used with the Process Device Configuration capability provided they have a DTM.

- **Loop** assets are collections of instruments, in a specified order, calibrated as one device. They are used to group together instruments used for a common purpose and reduce the overall number of calibrations that must be

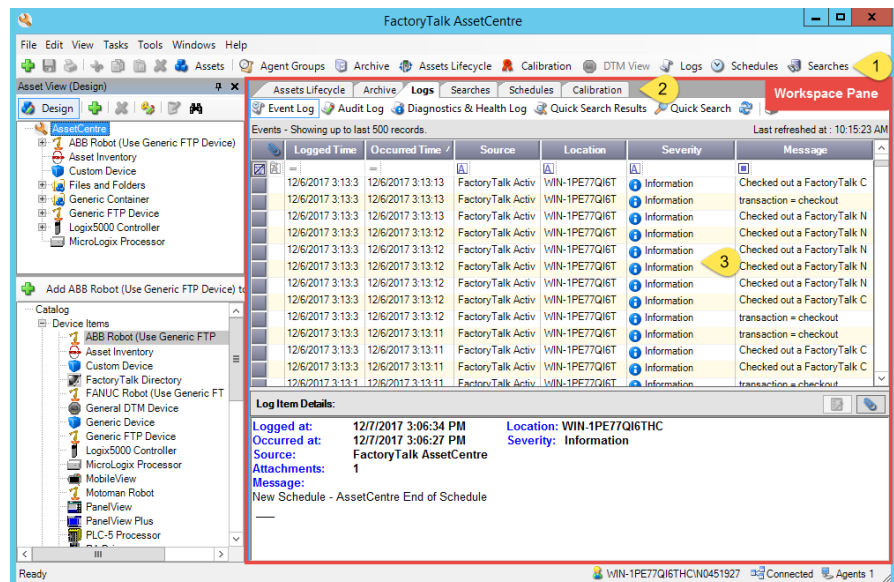
performed. For example, a temperature control loop may consist of an RTD sensor, a transmitter, and an indicator, where calibration is performed on the entire loop instead of the individual components. They can be placed under system and equipment process devices.

- **System** assets are the highest level grouping of calibration-related assets. They can be made up of other process device types (excluding test instruments), and even other systems. They can have their own calibration specifications or may just be used as a container to control scheduling of the associated devices. For example, a system record may consist of all the equipment, loops, and instruments that make up a plant HVAC system. They can be placed under system process devices.
- **Test Instrument** assets are used to calibrate other process devices. They are stand-alone devices that are never used as components of complex devices. To ensure traceability and to comply with ISO and other quality control processes, test instruments themselves must also be calibrated to NIST traceable standards. They can be placed under system, loop, and equipment process devices.

Tip: While containers and folders both contain assets, they are not interchangeable. Containers can hold ANY type of asset (including folders). Use a generic container to hold devices, process devices, and other associated assets. Folders or asset inventories can ONLY contain files, links, binders, and other folders.

Workspace pane

The **Workspace** Pane shows the information and controls for the FactoryTalk AssetCentre tools: Archive, Schedules, Logs, Searches, Agent Groups, and Address Book. Once a tool is selected, it appears on a tab in the **Workspace** Pane:



1. Click a button to show a tool in the **Workspace** Pane.

Alternatively, you can choose a tool on the **View** menu.








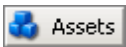
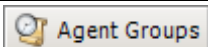
2. Tabs appear on the **Workspace** Pane for each tool that is open.
3. The tool that you are currently using is displayed in the Workspace pane.





Additional tabs may appear if you have purchased and installed additional FactoryTalk AssetCentre capabilities (such as Disaster Recovery or Calibration Management). Use the **Workspace** Pane to:

- Set up and run schedules. See [Quick Start 3: Set up Disaster Recovery schedules](#) on [page 51](#).
- View and search logs. See [Quick Start 4: View and search logs](#) on [page 59](#).
- Manage file versions in Archive. See [Quick Start 5: Open and edit files in Archive](#) on [page 69](#).
- Perform additional tasks depending on additional capabilities you have purchased and installed.

Toolbar

The following table lists the FactoryTalk AssetCentre client toolbar buttons and provides a brief description of each button's functions:

Button	Description
 New	Adds a new item such as an asset, schedule, search, or Address Book contact or group, depending on what is selected and has focus in the rest of the window. This button is unavailable if nothing can be added (for example, if the Asset View has focus, but is not in Design mode).
 Save	Available only when information (such as a schedule or search) has been edited, but not yet saved.
 Print	Available only when viewing a log. Prints either the selected records or all records listed.
 Cut	Combined with the Paste button, the Cut button moves an asset from one location in the tree to another. Select the asset, then click the Cut button. Click on the container in which you want to place the asset, then click the Paste button. The asset that was cut does not disappear from its original location until it is pasted in the new location.
 Copy	Combined with the Paste button, the Copy button duplicates an asset in the tree. First select the asset and click the Copy button. Next select the container in which you want to place the asset, then click the Paste button.
 Paste	Combined with the Cut (or Copy) button, the Paste button moves (or copies) an asset from one location in the tree to another. Select the asset, then click the Cut (or Copy) button. Click on the container in which you want to place the asset, then click the Paste button.
 Delete	Deletes the selected asset (if in Design mode), search, schedule, or Address Book contact or group. This has the same function as the Delete button on the Asset View toolbar, Search toolbar, and Schedules toolbar.
 Assets	Opens or shifts focus to the Asset View. This view contains the asset tree that you create to represent your system. For more information about the asset tree, see Quick Start 2: Design the asset tree on page 39 .
 Agent Groups	Opens the Agent Groups tab on which you can manage the agents into groups. If the tab is open, it brings the Agent Groups tab to the front.

 Archive	Opens or shifts focus to the Archive tab. Archive is FactoryTalk AssetCentre's source control tool that you will use to manage file versions. For more information, see Quick Start 5: Open and edit files in Archive on page 69 .
 Assets Lifecycle	Opens the Assets Lifecycle tab on which you can synchronize life-cycle information in the FactoryTalk AssetCentre server and client with the data on the Rockwell Automation life cycle website , or refresh life-cycle information in the AssetCentre client with the AssetCentre server.
 Calibration	Opens or shifts focus to the Calibration tab where you can view general and calibration information for the process device selected in the asset tree. Only available if the Calibration Management capability is activated.
 DTM View	Opens the DTM View tab for viewing and editing DTM information for the DTM device selected in the asset tree. Unlike the other tabs mentioned here, clicking this button if a DTM View tab is open does not simply bring the tab to the front. Instead it opens another DTM View tab. You can open multiple DTM View tabs, each one showing information for another device. Only available if the Process Device Configuration capability is activated and if the DTM catalog has been scanned at least once on this computer.
 Logs	Opens or shifts focus to the Logs tab. This tab allows you to view any of the logs -- the Audit Log, the Event Log, and the Diagnostics & Health Log. For more information, see Quick Start 4: View and search logs on page 59 .
 Schedules	Opens or shifts focus to the Schedules tab where you can set up scheduled operations such as Backup and Backup and Compare. For more information, see Quick Start 3: Set up Disaster Recovery schedules on page 51 .
 Searches	Opens or shifts focus to the Searches tab where you can search the logs or the Archive history. For more information, see Quick Start 4: View and search logs on page 59 .
 Properties	Shows the properties of the selected item: an asset in the Asset View or a contact in the Address Book, for example. For an asset, you can only edit the properties if the Asset View is in Design mode.
 Show Help	Shows the online help related to the part of the software you are currently using.

Menu bar

Any menu can be clicked or opened by holding down the **Alt** key and pressing the underlined letter in the menu name. For example, to show the **T**ools menu, press **Alt-t**. For information on any menu command, refer to the *About the Menu Bar* topic of the FactoryTalk AssetCentre online help.

Right-click menus

Right-click menus provide access to most functions in the FactoryTalk AssetCentre client and are available throughout the software. For example, right-click in the Asset View, on an asset in the Asset View, or in the Workspace Pane to see a list of functions particular to that item.

For information on a particular command on a right-click menu, refer to the online help and search for the command.

Status bar

The Status Bar at the bottom of the FactoryTalk AssetCentre window shows the currently logged on FactoryTalk user and the status of the connection to the

server. It also shows the number of FactoryTalk AssetCentre agents running in the system. If the server status is Disconnected see [If the client cannot communicate with the server](#) on [page 84](#).

About FactoryTalk AssetCentre Web Client

FactoryTalk AssetCentre supports the accessing of a FactoryTalk AssetCentre client through a web interface on computers and mobile devices. FactoryTalk AssetCentre Web Client supports several FactoryTalk AssetCentre client functions. The new capability allows you to:

- View archives and schedules in the asset tree
- View, run, and stop schedules
- View dashboards of the Backup and Backup and Compare schedule results
- View Event Log, Audit Log, and Diagnostics and Health Log
- View and run searches
- View agent groups

It is required that you use the SSL protocol with FactoryTalk AssetCentre Mobile Client. See [Step 6: Configure the SSL protocol](#) on [page 30](#).

Access FactoryTalk AssetCentre Web Client

To access FactoryTalk AssetCentre Web Client:

1. Open the device's browser, and type the following address:

```
https://FQDN/RockwellSoftware/AssetCentreWebClient
```

Tip: **FQDN** is the fully qualified domain name (FQDN) of the FactoryTalk AssetCentre Server computer.

2. On the FactoryTalk AssetCentre Web Client page, type the user name and the password.

Tip: Make sure to create a FactoryTalk Service Platform account and its password on the computer running FactoryTalk AssetCentre server. The account and password are used to log on to FactoryTalk AssetCentre Web Client.

3. Tap or click **Log in**.

Quick Start 1: Configure the system

After installing the FactoryTalk AssetCentre software, there are several steps you must perform to start using the software. The next several chapters of this guide take you through the steps required to quickly get results using FactoryTalk AssetCentre.

The main tasks necessary to begin using FactoryTalk AssetCentre are:

- [Quick Start 1: Configure the system](#) on [page 23](#)
- [Quick Start 2: Design the asset tree](#) on [page 39](#)
- [Quick Start 3: Set up Disaster Recovery schedules](#) on [page 51](#)
- [Quick Start 4: View and search logs](#) on [page 59](#)
- [Quick Start 5: Open and edit files in Archive](#) on [page 69](#)
- [Quick Start 6: Manage Rockwell Automation hardware life cycle](#) on [page 79](#)

This current chapter will concentrate only on the steps necessary to configure your FactoryTalk AssetCentre system.

Tip: If you have purchased additional FactoryTalk AssetCentre capabilities (such as Disaster Recovery or Calibration Management), see the online help for the *Get started with FactoryTalk AssetCentre* topic for the additional capabilities.

Quick Start steps for configuring the system

To configure your FactoryTalk AssetCentre system, you must perform the following steps:

- [Step 1: Add users to the FactoryTalk Directory](#) on [page 24](#)
- [Step 2: Add client computers](#) on [page 24](#)
- [Step 3: Set feature security for FactoryTalk AssetCentre](#) on [page 25](#)
- [Step 4: Add contacts to the FactoryTalk AssetCentre Address Book](#) on [page 28](#)
- [Step 5: Set up FactoryTalk AssetCentre database limitations](#) on [page 29](#)
- [Step 6: Configure the SSL protocol](#) on [page 30](#)
- [Step 7: Configure Windows Authentication](#) on [page 36](#)

Step 1: Add users to the FactoryTalk Directory

A user must have a FactoryTalk Directory user account to use FactoryTalk AssetCentre.

This step contains only basic instructions for using FactoryTalk Directory and FactoryTalk Security. For background information and information regarding more advanced procedures, please see the online help for the FactoryTalk Administration Console.

To add a user to FactoryTalk:

1. Start the FactoryTalk Administration Console.
2. Log onto the Network directory using a FactoryTalk Administrator account.
3. In the FactoryTalk Administration Console, open the **Users and Groups** folder.
4. Under the **Users and Groups** folder, right-click the **Users** folder, and click **New**.
5. Choose whether you want to create a new User or a Windows-Linked User. User accounts are visible only to the FactoryTalk system and their access is independent of Windows. A Windows-linked user is validated by Windows. See the FactoryTalk help topic *Account types* for more information. (A FactoryTalk Security account is the same as a User account.) To find this help topic, open the FactoryTalk Administration Console. Select **Help > Contents**. In the **Search** box, look up **Account types**.

If you choose to use Windows-linked accounts, consider using Windows-linked group accounts in place of Windows-linked user accounts wherever possible. This simplifies account administration, because FactoryTalk inherits any changes made to the Active Directory group (for example, adding the Active Directory user account of a new employee).

Tip: If you have users who need similar access to features of FactoryTalk AssetCentre, consider grouping users to make assigning security privileges easier. For example, you can group all of your electricians into an Electricians group, and then provide security access for them as a group.

For more detailed instructions on adding users and grouping users, refer to the *Manage users* topic of the FactoryTalk Administration Console online help.

Step 2: Add client computers

Before adding a client computer to the FactoryTalk AssetCentre system, install the FactoryTalk AssetCentre client software on a computer that meets the system requirements and is connected to the same network as the FactoryTalk AssetCentre server.

To add a client computer:

1. Install the FactoryTalk AssetCentre client on the computer:
 - a. Open Internet Explorer on the client computer. In the **Address** field of Internet Explorer, type the following address:

`http://servername/RockwellSoftware/AssetCentre`

where `servername` is the name of your FactoryTalk AssetCentre server.

For example, if your FactoryTalk AssetCentre server is called

`MYSERVER`, type:

`http://MYSERVER/RockwellSoftware/AssetCentre`.

If you are using SSL, then begin with `https://` instead of `http://`.

- b. Press **Enter**.

Internet Explorer shows a page from the server that allows you to install the FactoryTalk AssetCentre client software.

- c. Click **Install AssetCentre Client on this computer**.

2. On the **File Download - Security Warning** window, click **Run**.

Do not attempt to save the installation file — it will not run correctly from your local computer.

3. Follow the on-screen instructions to complete the installation.

For detailed instructions, select **Help > Installation Guide** to see the *FactoryTalk AssetCentre Installation Guide*.

During the installation, the FactoryTalk Services Platform will be installed and the computer will be added to the FactoryTalk Network Directory. If for some reason the client computer is not in the FactoryTalk Network Directory, use the FactoryTalk Administration Console to add it. See the online help for the FactoryTalk Administration Console for instructions on adding a computer.

Tip: If you have a significant number of computers for which you need to permit or restrict access, consider grouping them in the FactoryTalk Administration Console to make assigning security privileges easier. For example, you can group all of the computers used in offices away from the plant floor and restrict access to features that should be used only from computers stationed where the user can see the automation system directly.

Step 3: Configure security for FactoryTalk AssetCentre

By default, the Administrators and All Users groups in FactoryTalk Directory can perform any task in the FactoryTalk AssetCentre software. To deny specific users


the right to perform tasks in FactoryTalk AssetCentre, you must edit the Feature Security settings in the FactoryTalk Administration Console.

Important: Never explicitly deny rights to the All Users or Administrators group in FactoryTalk. Rather, set up specific user groups of your own and deny rights to those groups. Denying rights to All Users or Administrators could lock everyone out of the system and would deny rights in all FactoryTalk-enabled products.

To configure security settings:

1. In the **Explorer** pane of the FactoryTalk Administration Console, navigate to **System > Policies > Product Policies > FactoryTalk AssetCentre**.
2. Double-click **Feature Security**.

Important: Do not use the Server Settings properties in the FactoryTalk Administration Console to change server settings. Instead, go to **Start > All Programs > Rockwell Software > FactoryTalk AssetCentre Server > Server Settings** on the server computer. Changing server settings in the FactoryTalk Administration Console could enter conflicting information and prevent clients from connecting to the server. For more information, refer to the *Change server settings* topic of the FactoryTalk AssetCentre online help.

3. Click the feature (policy setting) for which you want to set permissions.
See [Policy settings and their meanings](#) on [page 26](#).
4. Next to the words **Configure Security**, click the browse button .
5. On the **Configure Securable Action** dialog box, select the user or group for whom you want to assign permissions. (If the user or group does not appear in the list, click **Add**, click **Show all**, select the user or group, and click **OK**.)
6. Click the appropriate box to allow or deny the user permission to the selected feature.
7. Click **OK**.

Tip: As a default, FactoryTalk AssetCentre uses Microsoft Windows file associations. To specify which software program will open a specific type of file, set file associations. See the *Set file associations* topic of the online help.

Policy settings and their meanings

The following table shows the policy settings and their meanings.

This policy setting...	Controls whether users can...
View Address Book	View the Address Book (which contains addresses for the purpose of sending automatic e-mail notifications).

Edit Address Book	Edit or add contacts and groups in the Address Book (which contains addresses for the purpose of sending automatic e-mail notifications).
Override Archive Check In	Check in a file regardless of who checked it out or from where it was checked out.
Configure Database Limitations	Configure the total maximum size of the AssetCentre database, the size warning levels, the maximum number of versions per archive asset, the maximum size of Event, Audit, and Diagnostics logs, and the database capacity status refresh rate.
Configure Asset Inventory Settings	Configure the settings in the Asset Inventory window.
Configure Archive Options Settings	Turn on or off the function that allows Logix Designer to perform archive activities, such as file check-in, without direct interaction with the FactoryTalk AssetCentre client.
Override Archive Undo Check Out	Undo a check out even if a different user checked the file out.
Override Removal of Local Copies	Choose to keep local copies of checked-in files on their computer. If this right is allowed, the user can keep local copies. If this right is denied, the user is not given this option.
Configure Personal Archive File Associations	Configure which software product launches when opening a particular type of file. If a personal file association is set, it will take precedence over the system file association.
Configure System Archive File Associations	Configure which software product launches when opening a particular type of file. This setting applies unless the user has specified a personal file association.
Configure Personal Archive Working Folders	Set a personal working folder for checking out files. For more information on working folders and personal working folders see the <i>FactoryTalk AssetCentre Client Help</i> .
Configure System Archive Working Folders	Set the system working folder to which all users check out files unless they have a personal working folder. For more information on working folders and system working folders, see the <i>FactoryTalk AssetCentre Client Help</i> .
Run Archive Database Cleanup Wizard	Run the Archive Database Cleanup Wizard to delete unused versions of files.
Allow Empty Comment at Check In	Leave the comment field empty as they check in an asset.
Configure Assets Lifecycle Sync	Synchronize life cycle information in the FactoryTalk AssetCentre server and client with the Rockwell Automation life cycle website .
Display Calibration Management Data	View Calibration Management data in FactoryTalk AssetCentre.
Perform Calibration Management	Access Calibration Management functionality in ProCalV5 software.
Administer Calibration Users	Administer users, groups, and permissions in ProCalV5 software. Note that this policy only determines if the user is automatically added to the Administrator group in the ProCalV5 software. Once the user is added to ProCalV5, changing this policy for an AssetCentre user does not change the user's ProCalV5 security permissions.
Switch to Design mode	Enter Design mode, in which the user can edit the asset tree.
View Event Log	Show the Event Log and run a search on the Event Log.
View Audit Log	Show the Audit Log and run a search on the Audit Log.
View Diagnostics and Health Log	Show the Diagnostics and Health Log and run a search on the Diagnostics and Health Log.
Change Diagnostics and Health Log Message	Change the status of or add a comment to a Diagnostics and Health Log record.
View Diagnostics and Health Log Status	View a status history for a Diagnostics and Health Log record.
Run Log Database Cleanup Wizard	Run the Log Database Cleanup Wizard to remove old records from the logs. Data can be exported and saved in a separate file.
Enable or Disable DTMs	Enable and disable DTMs in the DTM Catalog.
Edit DTM Network	Show the DTM Networks dialog box to edit the DTM network.
Run PDC Field Edition	Use the Process Device Configuration Field Edition software.
Create a schedule	Create a schedule.
Edit a schedule	Change existing schedules.
Delete a schedule	Delete schedules.
View a schedule	Show the Schedules tab.
Command a schedule	Issue commands to a schedule, such as making the schedule active or running the schedule immediately.
Create a search	Set up a new search to find entries matching specified criteria in one of the logs, in the Archive History, or in Archive Check Out Status information.

Step 4: Add contacts to the Address Book

Use the FactoryTalk AssetCentre Address Book tab to create contact information that the system uses to notify users about the progress and outcome of FactoryTalk AssetCentre schedules and other system-related events. You can then add contacts to groups (for example, `allelectricians@myplant.com`) if your existing mail system supports groups. This allows you to inform recipients about system events simultaneously.

Tip: You cannot import groups from another e-mail program. More than one user can create groups at the same time.

To create contacts and groups, you must be granted **View Address Book and Edit Address Book** permissions. See [Step 3: Set Feature Security for FactoryTalk AssetCentre](#) on [page 25](#).

To add contacts to the Address Book:

1. Start the FactoryTalk AssetCentre client.
2. Select **View > Address Book**.
3. Select **Tasks > Add New Address Book Contact** or click the **New** button (Keyboard users: Press **Ctrl-N**).
4. In the **New Contact name** dialog box, complete the **Contact** tab. You must enter a unique name for the contact that is not the same as any other contact or group name.
5. Click the **Internet** tab and complete it. You must enter an e-mail address for the contact to receive notifications.

Tip: If in your existing e-mail system you have a group that already has an e-mail address (for example, a group of electricians with the e-mail address `AllElectricians@MyCompany.com`), you can use that group's existing e-mail address. Simply create a contact and give it a name (for example, `Electricians`) and enter the group's e-mail address (`AllElectricians@MyCompany.com`) as the contact's default e-mail address. The individual e-mail addresses of the electricians in the group will not be added to the Address Book as contacts.

6. Click **OK**.

Once you have created Address Book contacts, you can add those contacts to Address Book groups. Groups cannot be imported from another e-mail program.

7. Click **Tasks > Add New Address Book Group**.

Tip: To add members to an existing rather than new group, see the online help. Select **Help > Contents**. Open the **Address Book** and click the **Modify contacts and groups** topic.

8. On the **Group** tab in the **Group Name** field, enter a name for the group.

9. Click **Select Members**.
10. In the **Contacts/Groups** list on the left of the **New Group** dialog box, select the contact or group to add to the group, and click **Select**.
11. Click **OK**.

Tip: To perform additional Address Book tasks (for example, to delete or modify groups or contacts), see the online help. Select **Help > Contents**, and open the *Addresses Book* chapter.

Step 5: Set up FactoryTalk AssetCentre database limitations

Use the **Options: Database Limitations** dialog box to specify the settings of database limitations, including:

- Total maximum size of the AssetCentre database
- Size warning levels
- Maximum number of versions per archive asset
- Maximum size of database table capturing logs
- Database capacity status refresh rate
- Email notification


Tip: Database limitation configuration is recommended but optional. You can use FactoryTalk AssetCentre without setting up database limitations.

To set up database limitations:

1. Start the FactoryTalk AssetCentre client.
2. Select **Tools > Options**.
3. Under **Category** on the left side of the dialog box, select **Database Limitations**.
4. Select the **Database Limitations Enabled** check box, and specify the settings as desired.

Tip: By default, the **Database Limitations Enabled** check box is not selected, and all the settings of database limitations are unavailable. To select the **Database Limitations Enabled** check box to configure all the settings, you must have **Configure Database Limitations** permission. See [Step 3: Set Feature Security for FactoryTalk AssetCentre](#) on [page 25](#).

The following table shows how to configure each setting for Database Limitations.

Settings	How to configure
Total maximum size of the AssetCentre database	Enter a value for the total maximum size of the AssetCentre database. No minimum value is required.
Size warning levels	Specify the percentage of database capacity as the Warning level or Critical level . The status of database usage appears in the status bar of the FactoryTalk AssetCentre client.
Maximum number of versions per archive asset	Enter a value for the maximum version number of an asset in archive. You can also configure the maximum number of versions per asset in Archive.
Maximum size of database table capturing logs	Enter a value for the maximum file size of Event Log, Audit Log, and Diagnostics Log. If the file size of any log exceeds its maximum size, FactoryTalk AssetCentre writes the log, and adds a new warning log about the current event log size exceeding its maximum size. When the Event, Audit, or Diagnostic and Health logs reach the maximum size, a warning message appears when you run the FactoryTalk AssetCentre client, indicating the log size status.
Database capacity status refresh rate	Enter a value to specify the frequency to refresh the database capacity status. The default value is 2. The minimum accepted value is 1, and 0 is not accepted. When the database capacity reaches the warning or critical level, or the Event, Audit, or Diagnostic and Health logs reach the maximum size, a warning message appears when the FactoryTalk AssetCentre client refreshes the database capacity status.
Email notification	Specify the email addresses to receive notifications when database size, asset version max, or log size reaches alarm level. Click the browse button  to select email address from Contacts and Groups address book dialog. If you set any value as 0 or higher than the maximum size, or leave any value blank, it is translated as unlimited.
SCAN to Proceed	Validate whether the current total database size, event log size, audit log size, diagnostics log size, and asset versions meet each own specified threshold. This operation is required when making any changes to the Database Limitations.

Not all situations during database limitation configuration are covered in this manual. For detailed information, refer to the FactoryTalk AssetCentre online help.

Step 6: Configure the SSL protocol

Important: Using the SSL protocol is an essential part of ensuring communications security. Without it, no communication, including logging on to the system, is encrypted.

Using the SSL protocol is required for FactoryTalk AssetCentre Web Client and recommended for the FactoryTalk AssetCentre server, clients, and agents.

The SSL configuration consists of the following steps:

- [Create an SSL certificate](#) on [page 31](#)
- [Import the SSL certificate to the Internet Information Services \(IIS\) Manager](#) on [page 31](#)
- [Add the certificate authority to client and agent computers](#) on [page 32](#)
- [Configure a site binding](#) on [page 32](#)
- [Enable secure communication between the server, client\(s\) and agent\(s\)](#) on [page 33](#)

- [Configure SSL settings for FactoryTalk AssetCentre Web Client](#) on [page 34](#)

Create an SSL certificate

In order to use the SSL protocol you need to have an SSL certificate.

When creating an SSL certificate, follow these recommendations:

- Use the public key infrastructure (PKI) available in your company for this purpose. If it is not possible, create a self-signed certificate.

For details, see

https://technet.microsoft.com/library/hh831637.aspx#Create_Certification

https://technet.microsoft.com/library/hh831637.aspx#Create_Certification.


- Make sure that the certificate meets the following requirements:
 - The minimum key size should be 2048 bits.
 - One of the following hash algorithms required for digital signature hash calculations should be used:
 - SHA-256
 - SHA-384
 - SHA-512

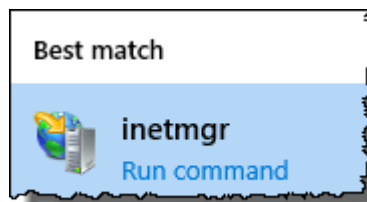
Import the SSL certificate to the Internet Information Services (IIS) Manager

To import the SSL certificate:

1. Open Internet Information Services (IIS) Manager on the FactoryTalk AssetCentre server computer:

On Windows Server 2016 and Windows Server 2012:

- a. On the taskbar click .
- b. In the search box, type *inetmgr*, and then press Enter.
- c. Click the best match result.




On Windows Server 2008 R2:

- d. Click **Start**.
- e. In the search box, type *inetmgr* and press ENTER.

The **Internet Information Services (IIS) Manager** window appears.

2. Under **Connections**, click the FactoryTalk AssetCentre server.
3. In **Features View**, double-click **Server Certificates**.
4. Under **Actions**, click **Import**.

The **Import Certificate** dialog box appears.

5. Under **Certificate file (.pfx)** click .

The **Open** dialog box appears.

6. Select your certificate file, and then click **Open**.
7. Under **Password**, type the certificate password, if it has been defined.
8. Under **Select Certificate Store**, select **Web Hosting**.
9. Click **OK**.

The certificate is listed under **Server Certificates**.

Add the certificate authority to client and agent computers

On all client and agent computers, add the certificate authority that issued the SSL certificate to the Trusted Root Certification Authorities certificate store.

For details, see

<https://msdn.microsoft.com/enus/windows/hardware/drivers/install/trusted-root-certificationauthorities-certificate-store> .

Configure a site binding


Prerequisites

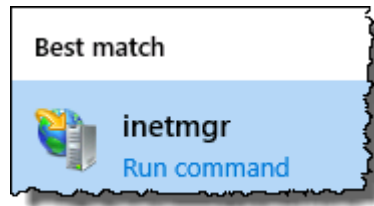
- Make sure that you have an SSL certificate.
See [Create an SSL certificate](#) on [page 31](#).

To configure a site binding:

1. Open Internet Information Services (IIS) Manager on the FactoryTalk AssetCentre server computer:

On Windows Server 2016 and Windows Server 2012:

- a. On the taskbar click .
- b. In the search box, type *inetmgr*, and then press Enter.
- c. Click the best match result.



On Windows Server 2008 R2:

- d. Click **Start**.
- e. In the search box, type *inetmgr* and press ENTER.

The **Internet Information Services (IIS) Manager** window appears.

2. Navigate to **localhost > Sites > Default Web Site**.
3. In the right pane, click **Bindings**.

The **Site Bindings** dialog box appears.

4. Click **Add**.

The **Add Site Binding** dialog box windows.

5. Configure the following settings:

For this option...	Do this...
Type	Select https
Host name	Type the fully qualified domain name (FQDN) of the FactoryTalk AssetCentre server.
SSL certificate	Select your SSL certificate. See Create an SSL certificate on page 31 .

6. Click **OK**.
7. In the **Site Bindings** dialog box, click **Close**.


Enable secure communication between the server, client(s) and agent(s)

Once you configured the SSL protocol, enable secure communication between the server, client(s) and agent(s) in the **Configure Server Settings Utility** window.

To enable secure communication:

1. Open the **Configure Server Settings Utility** window:

On Windows Server 2016 and Windows Server 2012:

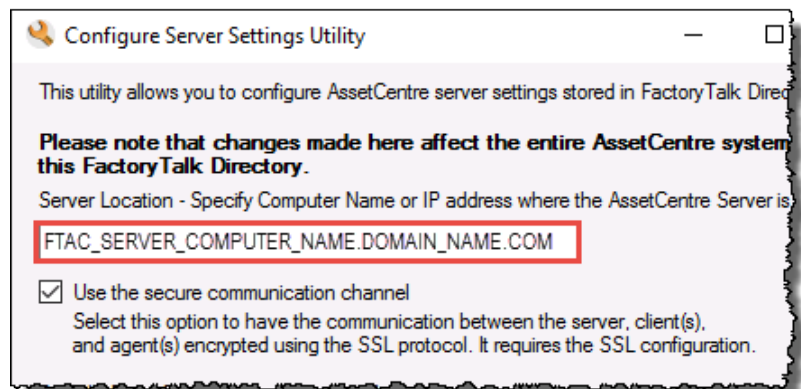
- a. On the taskbar click .
- b. Expand **Rockwell Software**, and then click **Server Settings**.

On Windows Server 2008 R2:

- a. Click **Start**.
- b. In the search box, type *Server Settings*, and then press Enter.
- c. In the search results list, click **Server Settings**.

The **Configure Server Settings Utility** window appears.

2. Under **Server Location**, type the fully qualified domain name (FQDN) of the FactoryTalk AssetCentre Server computer.



Note: Make sure that the FQDN is complete. Otherwise you may encounter some issues.
See Troubleshoot FactoryTalk AssetCentre.

3. Select the **Use the secure communication channel** option.
4. Click **Apply**.

**Configure SSL settings for
FactoryTalk AssetCentre Web Client****Before you begin**

Make sure that:

- You have an SSL certificate.

See [Create an SSL certificate](#) on [page 31](#)


- You have configured a https binding in the Internet Information Services (IIS) Manager.

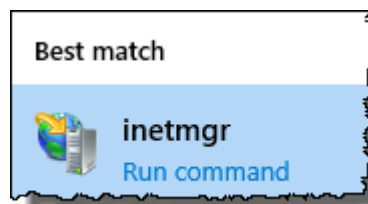
See [Configure a site binding](#) on [page 32](#).

To configure SSL settings for FactoryTalk AssetCentre Web Client:

1. Open Internet Information Services (IIS) Manager on the FactoryTalk AssetCentre server computer:

On Windows Server 2016 and Windows Server 2012:

- a. On the taskbar click .
- b. In the search box, type *inetmgr*, and then press Enter.
- c. Click the best match result.



On Windows Server 2008 R2:

- d. Click **Start**.
- e. In the search box, type *inetmgr* and press ENTER.

The **Internet Information Services (IIS) Manager** window appears.

2. Navigate to **localhost > Sites > Default Web Site > RockwellSoftware > AssetCenterWebClient**.
3. Under the **IIS** section, double-click **SSL Settings**.
4. Make sure the following options are selected:
 - **Require SSL**
Selecting this option will result in deactivating the HTTP protocol (with the default port 80). When you type *http://* in the web browser, it will be automatically redirected to *https://*.
 - **Ignore**
This option applies to the client certificates.

Step 7: Configure Windows Authentication

5. In the right pane, click **Apply**.

Windows Authentication is a secure way of authentication that uses the username and the password of the user logged on to the operating system. In the communication secured with Windows Authentication mode, the username and the password are sent between the client and the server in a strongly hashed form.

Windows Authentication may be enabled in corporate networks that use Microsoft Active Directory services as well as other ways to identify users.

By turning on Windows Authentication mode you increase the security of the communication between the FactoryTalk AssetCentre server, client(s) and agent(s) and prevent unauthorized users from accessing the FactoryTalk AssetCentre server.

Important: For the purposes of FactoryTalk AssetCentre, Windows Authentication mode should be enabled only in corporate networks that use Microsoft Active Directory services.

After you turn on Windows Authentication mode, the access to the page:

http(s)://accetcentre_server_full_name/rockwellsoftware/assetcentre

...will be secured from being accessed by anonymous users.

In order to access the page, the users will need to log on using their Windows username and password.

This section describes:


- [Turn on Windows Authentication mode in Internet Information Services \(IIS\)](#) on [page 36](#)

Turn on Windows Authentication mode in Internet Information Services (IIS)

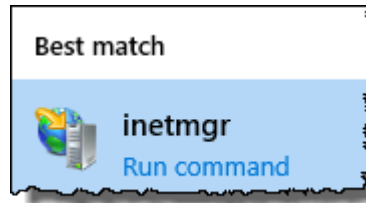
To turn on Windows Authentication mode in Internet Information Services (IIS):

1. Open Internet Information Services (IIS) Manager on the FactoryTalk AssetCentre server computer:

On Windows Server 2016 and Windows Server 2012:

- a. On the taskbar click .
- b. In the search box, type *inetmgr*, and then press Enter.

- c. Click the best match result.

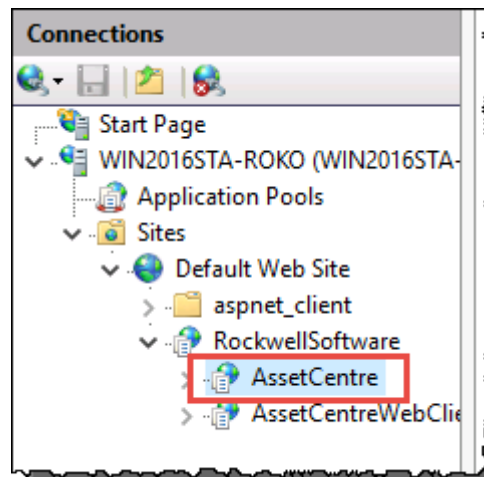


On Windows Server 2008 R2:

- d. Click **Start**.
- e. In the search box, type *inetmgr* and press ENTER.

The **Internet Information Services (IIS) Manager** window appears.

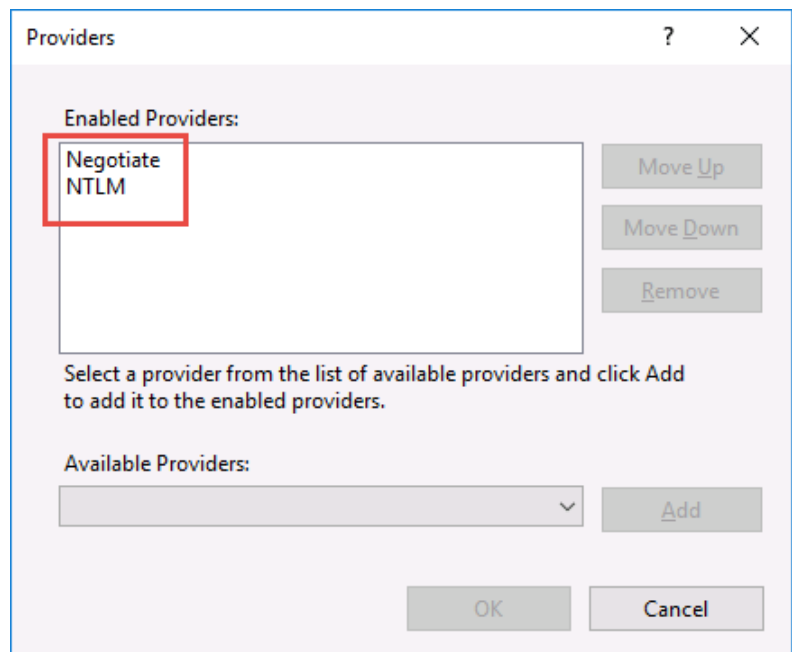
2. Under **Connections**, expand the tree, and then click **AssetCentre**.



3. In **Features View**, double-click **Authentication**.
4. Under **Authentication**, click **Windows Authentication**.
5. Under **Actions**, click **Providers**.

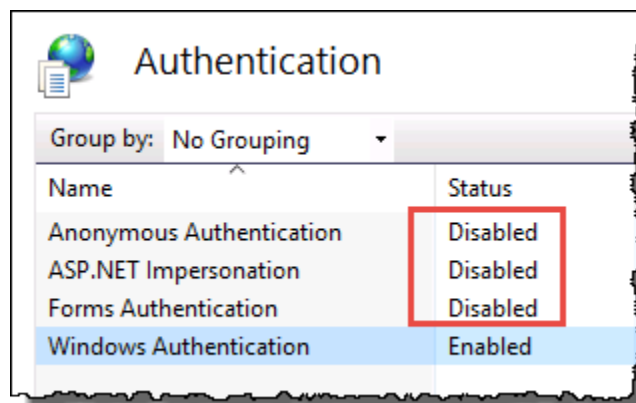
The **Providers** dialog box appears.

6. Make sure that you have the following providers selected in the order presented in the figure below.



If these providers are not listed, select each of them in the list under **Available Providers**, and then click **Add**.

7. Make sure that all other authentication modes listed in the pane under **Authentication** are disabled.



Quick Start 2: Design the asset tree

Everything that you do in FactoryTalk AssetCentre begins with an asset. The asset tree in the Asset View represents your plant including all the assets (anything from a device to a program to a procedure document) that you want to control, back up, or monitor. The asset tree provides you a method of organizing your plant assets in a logical fashion that makes sense to you (for example, by physical location, flow of materials, or machine type).

Quick Start steps for designing the asset tree

To design the asset tree, you must perform the following steps:

- [Step 1: Plan the organization of your asset tree](#) on [page 39](#)
- [Step 2: Add assets to the asset tree](#) on [page 41](#)
- [Step 3: Change security settings for an asset](#) on [page 48](#)

Step 1: Plan the organization of your asset tree

It is important to plan the organization of your asset tree in advance. The organization of the tree can impact your efficiency in applying security settings to assets and setting up Disaster Recovery schedules.

Tip: For background information to better understand the types of assets available in FactoryTalk AssetCentre and the use of the asset tree, see *About the Asset Catalog* and *About the Asset View* chapters in the online help.

You must be in Design mode to edit the tree. Only one user in the system at a time can be in Design mode.

Assets are listed in alphabetical order in the tree.

Security considerations

When initially added, an asset inherits the security settings of the container in which it is placed (and a container inherits the security settings of the container in which it is placed). First, set security on the root. Then add containers under the root and set security for those containers. Then add the next level of assets and containers, and so on.

Schedule considerations

Schedules are set up by selecting the asset to be scheduled from the Asset View. You can only select one asset when creating a schedule. If you want the schedule to

operate on multiple assets, place all those assets in a container in the asset tree. This container will be the starting point of the schedule. For example, if you want to backup the configuration files for a group of devices, place all those devices in a container in the Asset View.

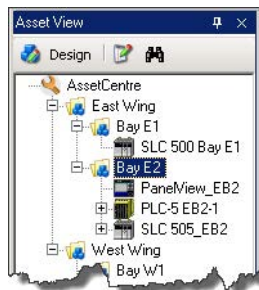
Only Rockwell Automation controller assets, Siemens SIMANTIC S5 and S7 processors, Rockwell Automation PanelView operator interfaces, PanelView Plus operator interfaces, MobileView operator interfaces, Rockwell Automation drives, remote computers, Custom Devices, RA Motor Control, Asset Inventory, FactoryTalk Directory, General DTM Device, Generic FTP Devices, and Remote Computer can be included in Disaster Recovery schedules (if you have the correct activation). Process Device assets cannot be included in Disaster Recovery schedules.

Organization

When you initially set up the asset tree, you will have to decide what will be the most useful organization for you. The examples below show three possible organizations:

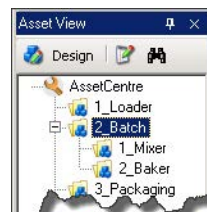
- **Physical location**

In this arrangement, assets are organized by their physical location in your plant.



- **Flow of materials**

In this arrangement assets are organized by the flow of materials in the production process. This may be particularly useful for continuous and batch processes.



Tip: Items in the tree are automatically organized alphabetically. If you want to force a certain order, use numbers in your asset names.

- **Machine type**

In this arrangement, assets are organized by the type of machine. You might further organize machines of the same type by location.



Step 2: Add assets to the asset tree

Assets are the heart of FactoryTalk AssetCentre. Anything you want the FactoryTalk AssetCentre system to manage must be included in the asset tree. On first use, all assets to be managed must be added to the asset tree.

There are rules that govern the location of the different types of assets that you can add to the asset tree:

- The root may contain any type of asset.
Best practice is to place only generic containers or folders directly under the root and use these to organize the tree in some useful way, perhaps by physical location or by function.
- A generic container may contain any type of asset.
- A device may contain files, binders, links, and folders.
- A folder or an asset inventory may contain files, binders, links, and folders.
- A file cannot contain any other assets.
- A link cannot contain any other assets.
- A binder cannot have any other assets placed under it.
Files are initially placed in the binder by specifying the files to include in the Add Binder dialog box and checking the binder in, not by placing files under the binder in the asset tree.
- A process device may contain files, links, folders, and binders.
- Some process devices may contain other process devices. (Process devices are generally used with the or only.)

Tip: When initially added, an asset inherits the security settings of the container in which it is placed (and a container inherits the security settings of the container in which it is placed). Take advantage of this inheritance by setting security for a container before placing assets inside that container. See [Step 3: Change security settings for an asset](#) on [page 48](#).

To add an asset to the tree, you must have:

- **Switch to Design Mode** permission. See [Step 3: Set Feature Security for FactoryTalk AssetCentre](#) on [page 25](#).
- **Create Children, Read, and Write** permissions for the container into which you want to add an asset. See [Step 3: Change security settings for an asset](#) on [page 48](#).

Work online and offline

You can add devices to the asset tree whether your FactoryTalk AssetCentre client computer is connected to the devices via a network or not. When connected to the devices, however, you can automatically acquire device information by browsing for the device. This is the preferred method in this manual. The client computer must be connected to the FactoryTalk AssetCentre Server to add devices to the asset tree.

Enter device information manually when:

- the asset cannot be identified by Rockwell Automation or third party network browsers. For example, a device not supported by FactoryTalk AssetCentre or the network browser would not be found when browsing the network.
- the asset has not been placed on the control network yet.
- the client workstation is working offline so it does not have access to the control network.

To enter device information manually when you are disconnected from the device network, see the online help. Select **Help > Contents**. Open the *Assets* chapter and click the **Associate a device in the Asset View with a networked device** topic.

To add assets:

1. To enter Design mode, on the Asset View toolbar, click the **Design** button (Keyboard users: Press **F3** to toggle Design mode on and off). If you cannot enter Design mode, see [If you can't enter Design Mode](#) on [page 85](#).
2. Click an asset in the Asset Catalog and drag it to the desired location in the asset tree.

Tip: Select the container into which you want to place the new asset and press **Ctrl-N**.

3. Enter the information for the asset. Be sure and complete the following fields:

- **Name.** Enter a unique name for the device.

Device Assets Names

Enter a unique and meaningful name for the device. This name will appear in the asset tree. The software defaults to the device type (for example, *FANUC Robot*). The name must be unique within the parent container. That is, you can have two devices with the same name in the asset tree, they just can't be in the same container. If you add a device into a container that already has a device of the same name, FactoryTalk AssetCentre will append a number (like _2) to the device name to ensure uniqueness.

Asset names can be a maximum of 260 characters. The characters \ / : * ? " < > | are not allowed. A space, tab, underscore (_) or dollar sign (\$) cannot be the first character in a name, but can be used elsewhere in the name. The following Microsoft Windows device names cannot be used as asset names, whether upper or lower case, with or without the colon: CON:, PRN:, AUX:, NUL:, COM1:, COM2:, COM3:, COM4:, COM5:, COM6:, COM7:, COM8:, COM9:, LPT1:, LPT2:, LPT3:, LPT4:, LPT5:, LPT6:, LPT7:, LPT8:, and LPT9. For example, *Auxiliary Line* would be a valid name whereas *Aux Line* would not.

- **Addressing Info.** For device assets, you must specify the device's network location. Click anywhere in the device's **Addressing Info** field and then click the **Browse** button. Then in the **Selecting Device for Asset Type** dialog box, browse the network to select the device you want to add and click **Select**.

If you are disconnected from the control network, you cannot specify the device address. Later, when you are connected to the control network, edit the device's properties to specify the device address.

- **Backup Data.** (Optional) You can specify the backup binder or file to use for Backup or Backup and Compare operations for Generic FTP devices, Siemens processors, Custom Device, RA Motor Control, and Asset Inventory. The Backup Data binder or file is used to store backup files and is used in Compare operations in Disaster Recovery schedules. To fill in this field, click in the field and then click the **Browse** button. The **Backup Data Browser** dialog box opens. Click **Help** on the dialog box for instructions.

In most cases when first configuring an asset, a backup binder or file does not exist yet. In this situation you can choose to leave Backup Data unspecified or you can specify a binder or file. For more information, refer to the *About the properties on the Device Properties dialog box* topic in the online help.

- **Configuration Data.** For device assets, you must add the files associated with the device to the asset tree. Simply adding the device to the asset tree does not take advantage of any of FactoryTalk AssetCentre's capabilities such as Disaster Recovery. Click anywhere in the device's **Configuration Data** field and then click the **Browse** button. Then in the **Configuration Data Browser** dialog box, select the desired file and click **OK**. (To add a new file to the device, click **Add**, select the desired file, click **Open**, select the file, and then click **OK**.)

Tip: The file or files specified in the **Configuration Data** field will be used as the master files for Disaster Recovery schedules. To learn about master files and Disaster Recovery, see [Quick Start 3: Set up Disaster Recovery schedules](#) on [page 51](#).

Adding a file to the asset tree automatically adds the file to **Archive**. Archive is FactoryTalk AssetCentre's source control tool that works like a library. Archive allows only one user at a time to check out, edit, and check in a file at a time. For more information on Archive, see [Quick Start 5: Open and edit files in Archive](#) on [page 69](#).

- **Agent Group.** Use the Agent Groups capability to manage the agents into groups. Click in the **Agent Group** field and then click the **Browse** button to select the agent group for the asset. When adding asset under the root, the default value of Agent Group is **System Default**. When adding asset under a container, the default value of Agent Group is **Inherit from parent: the parent container's Agent Group property**.
4. When the **(Device Type) Properties** dialog box is complete, click **OK**. For additional information about completing the fields for the device, click **Help**.

Tip: To learn about additional asset tasks (for example copying, deleting, moving, or renaming assets), refer to the online help. Select **Help > Contents**. Open the *Assets* chapter and click the desired topic.

Use Asset Inventory to add assets to the asset tree

FactoryTalk AssetCentre supports a new asset type, **Asset Inventory**. The **Asset Inventory** asset can be used to scan physical automation devices on the network. When you run a backup or backup and compare schedule on an Asset Inventory asset, the Asset Inventory agent service scans the connected devices and computers on the network and stores unique identification information about hardware, firmware, and software in the backup data. Once you have the Asset Inventory scanning result, you can add new assets from the scanning result to the asset tree. This is very helpful especially the first time you build the asset tree. For information about schedules, see [Step 4: Run schedules](#) on [page 57](#).

You need to open the **Asset Inventory** window first before adding assets to the asset tree. After running backup or backup and compare schedule on Asset Inventory, you can open the **Asset Inventory** window.

Important: You must enter design mode to add new assets to the asset tree.

To open the Asset Inventory window:

1. Select **View > Archive**, or click the **Archive** button.
2. In the asset tree, right-click the Asset Inventory backup file and select **Open**, or select the file in the asset tree and then at the top of the **Archive** tab, click the file link. The **File Retrieval Options** dialog box opens.
3. On the **File Retrieval Options** dialog box, keep the **Show in Asset Inventory Grid View** check box selected.

- If you want to open the Asset Inventory window in read-only mode, click the **Get** button. In read-only mode, you cannot edit the additional information or commission date for device assets. A read-only copy of the file is retrieved to the current working folder on your computer.

Tip: To open the Asset Inventory window in read-only mode, you can also right-click a version of Asset Inventory asset's backup data on the **History** tab of **Archive** and select **Asset Inventory View**.

- If you want to open the Asset Inventory window in editable mode, click the **Check Out** button. In editable mode, you can edit the additional information and commission date for device assets. A copy of the file is retrieved to the current working folder on your computer so that you can edit it.

Tip: Clear the **Show in Asset Inventory Grid View** check box to get or check out a file as a normal backup file, without opening it in the Asset Inventory window.

4. The **Asset Inventory** window opens.


Once the **Asset Inventory** window opens, you can add new assets to the asset tree.

To add new assets to the asset tree:


1. On the **Devices** tab in the **Asset Inventory** window, select the **Add** option.
2. Click the **SYNC** button.

Tip: Clicking the **SYNC** button doesn't add any new assets to the asset tree. It identifies assets in the scanning result that are new compared to assets on the asset tree. Make sure you are in design mode to proceed.

After clicking the **SYNC** button, assets on the **Devices** tab that:

- exist in the asset tree with the same properties appear dimmed. The check boxes before them are automatically selected.
 - exist in the asset tree with different properties appear dimmed. The check boxes before them are automatically selected. You can update these assets with different properties using the **Update** option.
 - don't exist in the asset tree can be added to the asset tree. The check boxes before the new assets are available.
3. Select the check boxes before the assets you want to add to the asset tree. Click the  **Add** button on the toolbar. The **Asset Inventory Add Asset Wizard** dialog box opens.
 4. On the **Asset Inventory Add Asset Wizard - Step 1 of 4** dialog box, enter the required information before proceeding.

- (Required) **Asset Type**

Click in the **Asset Type** field and click the browse button . On the **Select Asset Type** dialog box, select the asset type. Click **Select**.


Tip: Device assets that can be mapped to the corresponding asset type have the **Asset Type** field automatically filled. Otherwise, the **Asset Type** field is empty.

- (Optional) **Asset Name**

Click in the **Asset Name** field and type the asset name. The name must be unique within the parent container. That is, you can have two devices with the same name in the asset tree, they just can't be in the same container.

Tip: You can leave the **Asset Name** field blank. FactoryTalk AssetCentre automatically creates the asset name according to the asset type appended with a number (like _2).

- (Required) **Asset Location**

Click in the **Asset Location** field and click the browse button . On the **Select Asset Location** dialog box, select the node on the asset tree or click the **Add New Container** button to create a new generic container. Click **Select**.

Tip: The level an asset is added to the asset tree depends on which node you select in the asset tree structure. By default, the asset is added in the root. If you select a container, the asset is added to the container. If you select a non-container asset, the asset is added to the structure at the same level as other assets.

After **Asset Type** and **Asset Location** are specified, click **Next**.

Tip: You cannot proceed to the next step without specifying **Asset Type** and **Asset Location**.

5. On the **Asset Inventory Add Asset Wizard - Step 2 of 4** dialog box, review the details of the new assets that will be updated to the asset tree. Click **Start**.

Tip: To return to **Asset Inventory Add Asset Wizard - Step 1 of 4** to modify the asset type, name, or location, click **Back**.

6. On the **Asset Inventory Add Asset Wizard - Step 3 of 4** dialog box, a progress bar is shown while the adding operation is in process. If you want to cancel the operation, click **Abort**. Usually, this step takes a very short amount of time unless you are adding a large amount of assets.
7. When the adding process is complete, you can see result of the adding operation on the **Asset Inventory Add Asset Wizard - Step 4 of 4** dialog box. Click **Finish**.

To export the result, click **Export** to save the result as a .csv or .txt file.

Assets added to the asset tree appear dimmed on the **Devices** tab with check boxes selected before them.

For more information about Asset Inventory, refer to the FactoryTalk AssetCentre online help. Select **Help > Contents**, and open the *About the Asset Inventory window* chapter.

Step 3: Change security settings for an asset

Each asset in the asset tree has security settings controlling which users can perform what actions with that asset.

When initially added, an asset inherits the security settings of the container in which it is placed (and a container inherits the security settings of the container in which it is placed). That is, children inherit security permissions from their parents. You can assign explicit permissions to an asset, overriding the inherited permissions. You can also break the chain of inheritance for an asset so that it will not inherit permissions. For more information on inheritance see the FactoryTalk Security online help which is accessible from the **Security Settings** dialog box (referenced in the steps below).

If you move an asset, it retains its security settings. If you copy an asset, the copy does not retain the security settings of the original. Rather, the copy inherits the settings from its new parent container.

Tip: To change security settings for an asset, you must have **Switch to Design mode** permission. See [Step 3: Set feature security for FactoryTalk AssetCentre](#) on [page 25](#).
Keyboard users: Press **F3** to toggle Design mode on and off.

To change security settings for an asset:

1. While in Design mode, right-click the asset in the asset tree and select **Security**.
2. On the **Permissions** tab of the **Security Settings** dialog box, select whether you want to set permissions by **User** or by **Action**.
3. In the top pane, select either the user or the action for which you want to set security for the selected asset.
4. In the bottom pane select either the action (see the table below) or the user for which you want to set security and select or clear the **Allow** and **Deny** boxes accordingly. For more detailed information on using the dialog box and FactoryTalk Security, click **Help**.

This action...	Allows you to...
AssetCentre	
CheckOut - CheckIn	Check out or check in files associated with the selected asset.

Get	Get a copy of the file or files associated with the selected asset from Archive .
Label	Apply a descriptive Label to a version of a file associated with the selected asset in Archive .
Pin	Pin a version of a file associated with the selected asset.
Promote	Store an old version of the file as the most recent version.
Set Store Latest Version	Specify that only the most recent version of the file associated with the selected file asset should be retained.
Set Working Folder	Set the working folder for files associated with the selected asset.
Undo CheckOut	Undo a check-out operation for files associated with the selected asset. See the online help. Select Help > Contents . Open the <i>Archive</i> chapter and click the Undo a check-out topic.
Common	
Configure Security	Change security settings for the selected asset.
Create Children	Add assets underneath the selected asset (only if the selected asset is a container or device-type asset).
Delete	Delete the selected asset from the asset tree.
Execute	This setting is not applicable in this release of the FactoryTalk AssetCentre software.
List Children	Show children of the selected asset. If a user does not have this right, they will not be able to expand the selected asset to see assets that it contains. If you set this right to Allow , also set the Read right for this asset to Allow .
Read	Show the selected asset in the asset tree. Show the selected asset's properties.
Write	Change the selected asset's properties.

Tip: For more information on any of the Archive tasks listed in the first section of this table, see [Quick Start 5: Open and edit files in Archive](#) on [page 69](#).
To learn about additional asset tasks (for example copying, deleting, moving, or renaming assets), refer to the online help. Select **Help > Contents**. Open the *Assets* chapter and click the desired topic.

Quick Start 3: Set up Disaster Recovery schedules

FactoryTalk AssetCentre allows you to create certain types of scheduled operations, the results of which (whether or not the operation completed successfully) can be e-mailed to the desired recipients. Currently, FactoryTalk AssetCentre offers two types of scheduled operations beyond scheduling searches — Device Monitor and Disaster Recovery. The Disaster Recovery capability ensures quick and accurate file recovery by verifying your devices' program and configuration files against protected master files.

A master file is a designated version of an asset's configuration data file. A master file may initially be uploaded from the physical device such as a controller, processor, or robot, or it may be saved directly from the programming software (such as RSLogix 500). A master file is added to FactoryTalk AssetCentre for backup in **Archive** and is required for some FactoryTalk AssetCentre functions such as Disaster Recovery Backup and Compare schedules (where the file in the physical asset is backed up and compared to the master file stored in Archive so the differences can be reported).

Disaster Recovery provides two types of operations:

- **Backup.** Stores a backup copy of files associated with a number of devices, including Rockwell Automation devices, Siemens S7 processors, FTP devices including Robots, and more.
- **Backup and Compare.** Retrieves a copy of the files associated with a device asset. If differences are found and you choose to store the uploaded device files, the retrieved copy of files associated with the device asset are promoted as the new master file stored in **Archive**.

Scheduled events for Rockwell Automation Logix 5000 processors will fail if FactoryTalk Security is enabled for that devices' programming software (RSLogix 5000 versions 16 and earlier). The problem is fixed in RSLogix 5000 versions higher than 16. For RSLogix 5000 versions 16 and earlier, running scheduled events requires single sign-on for these versions. This issue does not affect other device's schedules (such as robots or PanelView devices). If a schedule contains both Logix 5000 processors and other devices, the scheduled event will only fail for those Logix 5000 processors for which FactoryTalk Security is enabled in the programming software; the event will complete for the other devices.

To configure the system so that scheduled operations will succeed even with security enabled in the RSLogix software, see the online help. Select **Help > Contents**. Open the *Welcome to FactoryTalk AssetCentre* chapter and click the **About the configuration for security-enabled RSLogix products** topic.

Also, activation is required for Disaster Recovery. For information regarding the activation required, see the online help. Select **Help > Contents**. Open the *Welcome to FactoryTalk AssetCentre* chapter and click the **Activation in FactoryTalk AssetCentre** topic.

Tip: To create scheduled searches instead of scheduled Disaster Recovery operations, see [Step 2: Create a search](#) on [page 62](#).

Quick Start steps for setting up schedules

To set up schedules, you must perform the following steps:

- [Step 1: Set up Agent Groups and agent computers in them](#) on [page 52](#)
- [Step 2: Create a schedule for the desired Disaster Recovery operation](#) on [page 54](#)
- [Step 3: Set up recipient lists for schedule results](#) on [page 55](#)
- [Step 4: Run schedules](#) on [page 57](#)

Step 1: Set up Agent Groups and agent computers in them

FactoryTalk AssetCentre uses agents to perform Disaster Recovery operations. Agents are programs that communicate with the FactoryTalk AssetCentre server and perform tasks on behalf of the server. Agents allow work to be distributed and shared among multiple computers to spread processing load and speed up operations. When a server needs an agent to perform a task, it locates the computer running the operation and assigns the task to that agent. The agent then reports the task's completion to the server.

FactoryTalk AssetCentre Agent Groups is a plug-in that helps you manage the agents into groups. With this plug-in, the agent computers that are connected to the same FactoryTalk AssetCentre server do not need to have the same configuration. This plug-in allows you to:

- Create agent groups, assign agent computers to the agent groups, and identify an agent group for an asset
- Assign backup and compare schedule tasks on an asset to the agent computers that belong to the asset's agent group
- Monitor the status of agent computers in the **Agent Status** pane, the **Agent Group Creation and Agent Assignment** pane, and the **Assets per Agent Group** pane.

This manual covers operations configuring Agent Groups and agent computers within those groups. To add a physical agent computer into FactoryTalk


AssetCentre system instead of managing agent computers in agent groups, see the online help. Select **Help > Contents**. Open the *Administration* chapter and click the **Add an agent computer** topic.

To learn about more Agent Groups configurations (for example, delete and rename an agent group, edit agent group properties, delete an agent computer, edit agent computer properties, move an agent computer, and move an asset from one agent group in to another) not covered in this manual, refer to the online help. Select **Help > Contents**. Open the *Agent Groups* chapter and click the desired topic.

Create an agent group

Agent Groups plug-in manages the usage of agents. By default, there is one System Default agent group, which cannot be renamed or deleted. The System Default agent group is used for scheduled searches, and by default for any Disaster Recovery tasks. If you need to create a new agent group, follow the steps below.

To create an agent group:

1. If you are not in it, enter Design mode.
2. On the **Menu** bar, click **View > Agent Groups** (or click the **Agent Groups** button).
3. Click the **Add Agent Group** button  on the **Agent group Creation and Agent Assignment** toolbar. The **Add an Agent Group** dialog box opens.

Tip: You can also right-click anywhere in **Agent Group Creation and Agent Assignment** pane and select **Add Agent Group**.

4. On the **Add an Agent Group** dialog box, enter the name and the description for the agent group. Click **OK**.


Tip: The maximum number of agent groups which you can create depends on your licensed agent group capacity. By default, you can create one agent group in addition to the existing System Default agent group.

Create an agent computer

You can create an agent computer in Agent Groups to monitor the physical agent computers.

To create an agent computer:

1. If you are not in it, enter Design mode.

2. On the **Menu** bar, click **View > Agent Groups** (or click the **Agent Groups** button).
3. Select an agent group, or an agent computer under the group where you want to add the agent computer to. Otherwise, the agent computer will be created under System Default agent group.
4. Click the **Add Agent Computer** button  on the **Agent Group Creation and Agent Assignment** toolbar. The **Add an Agent Computer** dialog box opens.

Tip: You can also right-click the agent group and select **Add Agent Computer**.

5. On the **Add an Agent Computer** dialog box, enter the name, location and the description for the agent computer.

You can click the **Connect** button to check whether the FactoryTalk AssetCentre Server service can connect to the agent computer.

6. Click **OK**.

Step 2: Create a schedule for the desired Disaster Recovery operation

You can set up either a Backup or Backup and Compare Disaster Recovery operation when you create a schedule.

Tip: To create schedules, you must have **Create a new schedule**, **Edit a schedule**, and **Command a schedule** permissions. See [Step 3: Set Feature Security for FactoryTalk AssetCentre](#) on [page 25](#).

To create a schedule:

1. In the asset tree, select the container or device for which you want to schedule an operation.

Tip: Multiple assets can be included in the same scheduled operation by creating a scheduled operation for a container. For example, a single container may contain multiple controllers. Scheduling a Backup operation for the container backs up all of the devices in that container in one operation.

For all of a device's schedule properties to be available for modification, make sure each device to be added to a schedule has its Configuration Data defined in the device's properties. The Configuration Data will be used to specify the master file for a Disaster Recovery schedule. See [Step 2: Add assets to the asset tree](#) on [page 39](#).

2. Select **View > Schedules** (or click the **Schedules** button).
3. Click the **New** button (Keyboard users: Press **Ctrl-N**).
4. Complete the **New Schedule Wizard: Step 1 Schedule Properties** dialog box and then click **Next**.

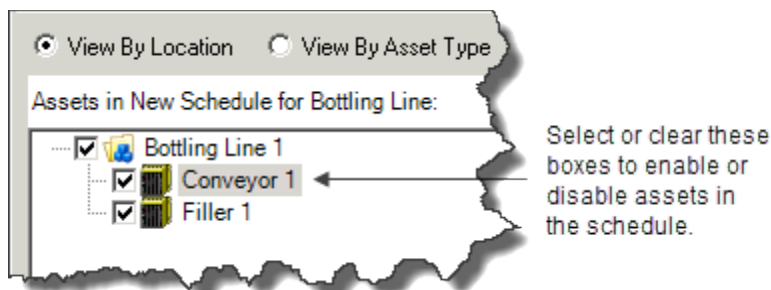
You must enter a unique name for the schedule.

If you have more than one e-mail address you want to include, separate the addresses in the **Completion Email List** field with semicolons (;), or, if you have **View Address Book** permission, select the contacts or groups from the FactoryTalk Address Book. The report sent from this field is the End of Schedule Report. For more information about the End of Schedule report, see [Step 2: Set up recipient lists for schedule results](#) on [page 55](#). For more information on a particular field, click **Help**.

5. Complete the **New Schedule Wizard: Step 2 Recurrence Pattern** dialog box and click **Next**.

To create a start time that does not begin on the hour or half hour, type the time (and AM or PM) in the field. Be aware that it is possible to create a schedule that will not run on a specific date. For example, if you choose to have a schedule run on the 31st day of every month, it will not execute in months that do not have 31 days. For more information on a particular field, click **Help**.

6. Complete the **New Schedule Wizard: Step 3 Operation Properties** dialog box. In the tree on the left side of the dialog box, check boxes appear selected next to each asset in the schedule. Clear a box to not include that asset in the schedule.



Properties for the selected device appear on the right side of the dialog box. For help completing the shown properties for the selected device, click **Help**.

The schedule you created will be active unless you clear the **Activate the Schedule** box. For more information on a particular field, click **Help**.

7. Click **Finished**.

Step 3: Set up recipient lists for schedule results

There are two different types of schedule reports you can send to specified recipients when a schedule completes:

- **End of Schedule report.** This general report summarizes information such as a Backup and Compare schedule's start and stop times and whether there were any differences between the contents of the physical device and the asset's master file stored in **Archive**. This report is set up through the **Schedules** tab.
- **Backup report or Backup and Compare report.** These more detailed, operation-specific reports include information such as asset and hardware details, the agent computer that ran the schedule, and the name and location of the master file used in a Compare. For Backup and Compare operations, the Backup and Compare report indicates whether or not differences were found. To include the detail of what these differences were, attach the Compare Report file to the e-mail notifications. Both the Backup report and Backup and Compare report are set up through an asset's scheduled operation properties.

Tip: To send schedule results, you must have **Command a schedule** and **Edit a schedule** permissions. See [Step 3: Set Feature Security for FactoryTalk AssetCentre](#) on [page 25](#).

Send an End of Schedule report

To send an End of Schedule report at the end of a schedule:

1. On the **Schedules** tab, click in the desired schedule's **Completion Email List** field and then click the **Browse** button. The schedule must be inactive to change the e-mail address, that is, the Active check box must be cleared.
2. Complete the **Contacts** dialog box.
3. To avoid scrolling the entire list, begin typing the last name of the contact or the name of the group. You can double-click the contact or group to add it to the list of recipients at the bottom of the dialog box. For information on adding a new contact, see [Step 4: Add contacts to the Address Book](#) on [page 28](#).
4. Click **OK**.

Send an operation-specific report

To send a Backup report or Backup and Compare report at the end of a schedule:

1. On the **Schedules** tab, select the schedule containing the asset for which you want to send a report.
2. To select the asset associated with the schedule and complete its e-mail (and other) operation properties, see the online help. Select **Help > Content**. Open the *Schedules* chapter and click the **Modify scheduled operation properties** topic.

Tip: After a Backup and Compare operation completes, if no differences are found, the Compare Report file is attached to e-mail notifications if, in the device properties under **Attach Report to email**, you set the **Event Completed** field to **True**. If differences are found, the Compare Report file is attached to e-mail notifications if you set the **Event Compare Differences Detected** field to **True**. See the online help. Select **Help > Content**. Open the *Schedules* chapter and click the **Modify scheduled operation properties** topic.

Step 4: Run schedules

You can activate a schedule so that it runs at its next scheduled time. You did this automatically if you selected the **Activate the Schedule** box in the wizard when you created the schedule. You can also activate schedules from the **Schedules** tab.

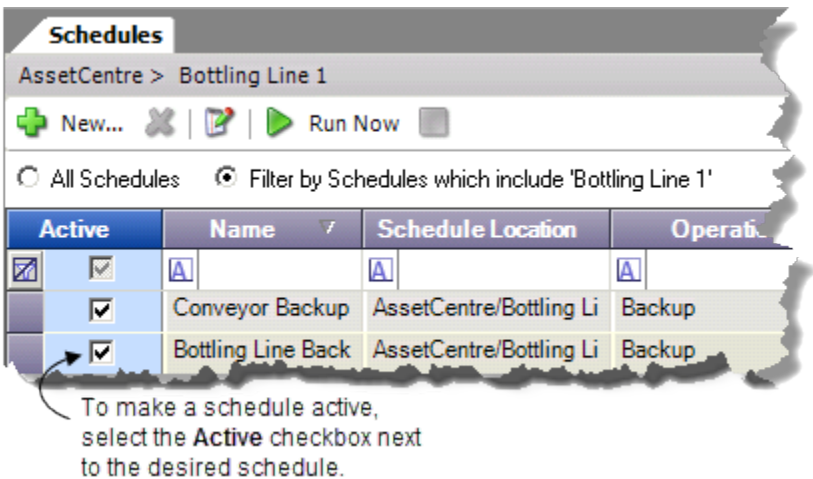
To run a schedule immediately, you can run schedules manually. Choosing to run a schedule manually immediately runs the schedule and sends e-mail notifications to your recipient list instead of waiting for the operation's next run time. Running a schedule manually does not affect that schedule's next run time.

Tip: To run schedules, you must have **Command a schedule** permission. To activate schedules, you must have **Edit a schedule** permission. See [Step 3: Set Feature Security for FactoryTalk AssetCentre](#) on [page 25](#).

Run schedules by making them active

To activate an existing schedule that you did not activate when you created the schedule:

- On the **Schedules** tab next to the schedule you want to activate, select the **Active** check box. If the selected schedule is to run daily at 4:00 P.M., the schedule will run next at 4:00 P.M. today (or 4:00 P.M. tomorrow if it is already later than 4:00 P.M. today).



Run schedules manually

To run a schedule immediately without waiting for its next scheduled run time:

1. You cannot manually run a schedule that has Running status, so on the **Schedules** tab, select a schedule with Waiting to Run status.
2. Click the **Run Now** button.
3. Once the schedule is run manually, it returns to Waiting to Run status. If running the schedule manually causes the schedule to run through its start time, FactoryTalk AssetCentre does not attempt to run the previously scheduled operation. Instead, the message *The schedule has tripped but didn't run because it is already running* is logged to the AssetCentre Event Log and the schedule waits to run again at its next start time.

Tip: When you move, copy, or delete assets in the asset tree, the schedules for those assets are also moved, copied, or deleted. To learn about the impacts moving, copying, and deleting assets have on schedules, refer to the online help. Select **Help > Contents**. Open the *Schedules* chapter and click the **Schedule changes when assets are moved, copied, deleted or renamed** topic.

To learn about additional schedule tasks (for example, stopping schedules, changing schedule run times, setting asset defaults for schedules, or renaming, filtering, and deleting schedules) not covered in this manual, refer to the online help. Select **Help > Contents**. Open the *Schedules* chapter and click the desired topic.

Quick Start 4: View and search logs

FactoryTalk AssetCentre offers three different logs:

- **Event Log.** This log shows database information regarding events that occur in the system. Events are generally system-initiated, for example an upload occurred, or a scheduled task completed. Event records are generated by FactoryTalk-enabled products.
- **Audit Log.** This log shows database information regarding actions users perform in the system, such as making edits to an RSLogix 5000 project or opening or closing such a software product. Audit records are generated by FactoryTalk-enabled products.
- **Diagnostics & Health Log.** The Diagnostics and Health Log provides information about the condition of automation devices. For example, a monitoring software product, such as RSNetWorx MD, detects a problem with a device on the automation network. It reports the problem and logs the information in the Diagnostics and Health Log.

Tip: Initially, only previously existing data appears in the Diagnostics and Health Log if that data was imported from the RSMACC Network Health Solution. This data is not updated by FactoryTalk AssetCentre. New data is logged in the Diagnostics and Health Log only if RSNetWorx MD is installed on your system.

You can search for and show specified records from one log at a time. For example, you could search for log entries where a specific user performed a task on a specific computer.

You can perform searches in two different manners:

- **Scheduled searches** are used to execute a search on a recurring basis and works well for detecting specific conditions and user behaviors in log data. For instance, you can create a scheduled search to detect unsafe programming practices among your maintenance staff by searching the Audit Log for edits made to program files at the end of each shift. You can run scheduled searches manually to show search results immediately. Scheduled search results can be delivered via e-mail. Search results can be printed and saved in .PDF format.
- **Unscheduled searches** are used for one-time purposes or when there is an immediate need, such as searching the Audit Log to determine if anyone has

made a change in a control system that was working fine a few hours ago, but now is down and preventing production.

Tip: In addition to searching logs, you can search the Archive History Log and the Archive Check Out Status.
To perform a quick search without complex conditions instead of the full searches described in this manual, see the online help. Select **Help > Contents**. Open the *Logs* chapter and click the **Perform a Quick Search on a log** topic.

Quick Start steps for viewing and searching logs

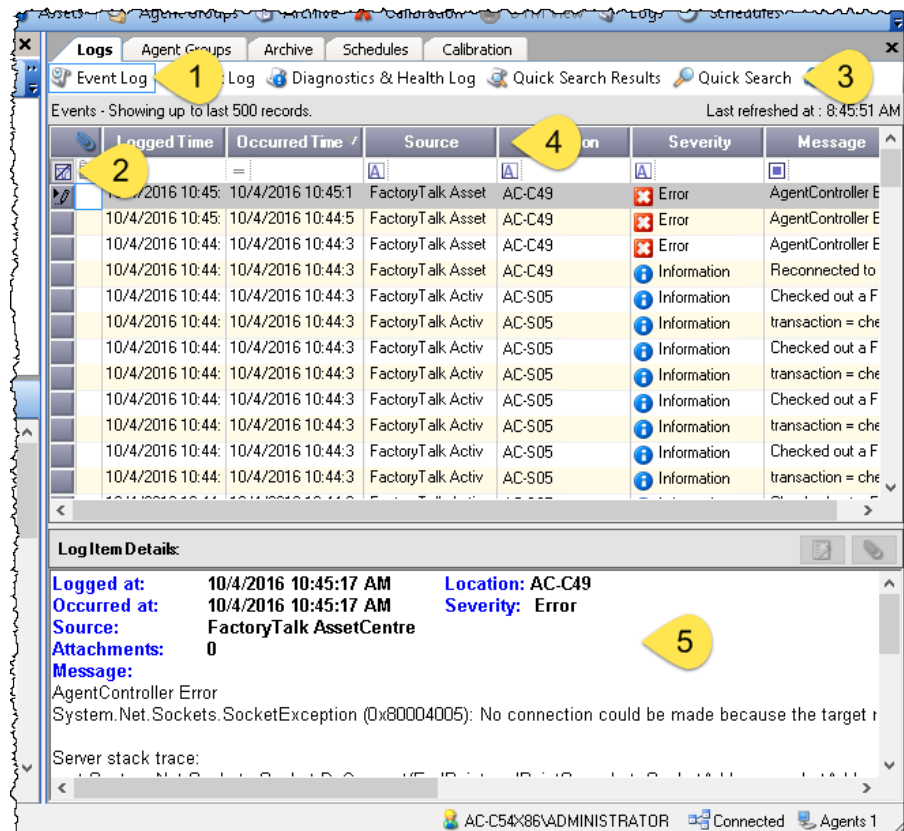
To set up searches, you can view logs and then perform the steps to set up and run searches:

- [Step 1: View logs](#) on [page 60](#)
- [Step 2: Create a search](#) on [page 62](#)
- [Step 3: Set search security](#) on [page 66](#)
- [Step 4: Run searches](#) on [page 67](#)
- [Step 5: View and print search results](#) on [page 68](#)

Step 1: View logs

Viewing a particular log shows the latest entries for that log only. If no data appears in the log, see [If no data appears in a log on page 90](#).

Tip: To view the desired log, you must be granted **View Audit Log**, **View Event Log**, or **View Diagnostics and Health Log** permission. If you do not have rights to view the desired log, the message *You do not have permission to view the selected log* will appear. See [Step 3: Set Feature Security for FactoryTalk AssetCentre](#) on page 25.



1. When you click a log button, the newest log entries for the selected log appear.
2. Use the filter fields to limit the items shown in the log. To filter fields, see the online help.

Click **Help > Contents**. Open the *Logs* chapter and click the **Filter log records** topic.

3. To perform a quick search on a log, see the online help.

Click **Help > Contents**. Open the *Logs* chapter and click **Perform a quick search** on a log topic.

4. Use the column headings to sort and arrange the log data. See the online help.


Click **Help > Contents**. Open the *Logs* chapter and click the **Sort and arrange log records** topic.

5. When you click a log entry, its contents is shown here in the **Details** pane.

To view logs:

1. Select **View > Logs**.
2. To view the desired log:
 - Select **View > Audit Log** (or click the **Audit Log** button).
 - Select **View > Event Log** (or click the **Event Log** button).
 - Select **View > Diagnostics & Health Log** (or click the **Diagnostics & Health Log** button).

To learn about the data fields shown in each log, click **Help** while the desired log is shown.

3. To show the contents of a log entry in the **Log Item Details** pane, click the log entry.
4. To update the shown log with any additional records, click the **Refresh** button . This updates the records in the log with events that occurred in your system since the log display was last refreshed. The log display is automatically refreshed at the rate determined in the client software settings. To change the number of seconds between automatic refreshes, see the online help. Select **Help > Contents**. Open the *Logs* chapter and click the **Change the refresh rate and number of shown records** topic.

Tip: To learn about additional log tasks (for example, sorting, filtering, printing, showing attachments, or changing the status of a Diagnostics & Health Log record) see the online help. Select **Help > Contents**. Open the *Logs* chapter and click the desired topic.

Step 2: Create a search

Use FactoryTalk AssetCentre Searches to show specified log records from the Event Log, Audit Log, Diagnostics and Health Log, the Archive History, or the Archive Check Out Status. Search results can be based on any column of data in a log and are generated based on complex conditions that you set.

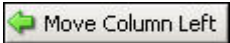


Tip: To create unscheduled searches, you must have **Create a Search** permission. To create scheduled searches, you must also be granted **Create a Schedule**, **Edit a Schedule**, **View a Schedule**, and **Command a schedule** permissions. See [Step 3: Set Feature Security for FactoryTalk AssetCentre](#) on [page 25](#).


To create a search:

1. Select **View > Searches** (or click the **Searches** button).
2. Click the **New** button (Keyboard users: Press **Ctrl-N**).
3. Complete the Search Properties page of the **New Search Wizard** dialog box. Be sure to enter a unique name for the search and select its data source (the log you want to search). For information to complete any of the fields, click **Help**.
4. To create an unscheduled search for the selected log, click **Finished** and go to Step 6.
5. To create a scheduled search to run at a later time, click **Schedule**, complete the **New Schedule Wizard: Step 2 Timing Properties** dialog box.

To create a start time that does not begin on the hour or half hour, type the time (and AM or PM) in the field. Be aware that it is possible to create a search that will not run on a specific date. For example, if you choose to have a search run on the 31st day of every month, it will not execute in months that do not have 31 days. For more information on a particular field, click **Help**. When the dialog box is complete, click **Finished**.

6. To configure how the search results will appear, complete the **Source and Display** tab. If you do not complete this tab, the default format will be used for the search results. The following table lists this tab's buttons and options:

Button or graphic	Description
 Move Column Left	Move the selected column one column to the left. Columns appear in the search results report in the order in which they are shown here. The columns of data available vary depending on the log you are searching. Sort precedence is determined by column display order. For example, if you want to sort the results by user name and then logged time, place User Name as the first column and Logged Time as the second column.
 Move Column Right.	Move the selected column one column to the right. Columns are sorted in the order in which they are shown. The columns shown vary depending on the log you are searching. For example, if you want to sort the results by user name and then logged time, place User Name as the first column and Logged Time as the second column.
 Show all Columns	Show all of the selected log's columns in the search results. This is helpful if you have de-selected some of the columns and want to re-select all of the columns without doing so manually.

	Show none of the selected log's columns in the search results. This is helpful if you want to show very few columns because you can deselect all of the columns and then select only those that you want.
Show (row heading)	Show the log's selected data fields in the search results. In the Show row beneath the column heading, select the checkbox for each field of data to show in the search results.
Sort (row heading)	Select the shown data fields (above) to sort the search results. In the Sort row beneath the column heading, click the cell to select the desired sort order (Ascending, Descending, or No Sorting). Columns are sorted in the order in which they are shown. To change column order, use the Move Column buttons described above.
Display all rows	In the search results, show all records of the source log that meet the search criteria.
Display only the first (number) rows	In the search results, limit the matching records shown up to the number indicated.
Tabular style	Tabular style arranges each record with column-style headings.
Card style	Card style arranges each record with row-style headings.

- To create or modify the search criteria for the selected search definition, complete the **Conditions** tab. The conditions you create determine the log records that will appear in the search results. For example, you can create a condition to include only those search results logged before or after a specific date and time. If you do not complete this tab, there will be no conditions placed on the log records returned in the search results. That is, the search will return all records.

How FactoryTalk AssetCentre Evaluates Search Conditions

Evaluating ungrouped conditions is pretty straightforward. FactoryTalk AssetCentre evaluates conditions from top to bottom. Place conditions in the order you want them evaluated by using the **Move Up** and **Move Down** buttons.

More complicated expressions can have a different meaning depending on how the elements are grouped. With no grouping, FactoryTalk AssetCentre evaluates first the AND operators and then the OR operators. Conditions grouped with parenthesis override this, so anything in parenthesis is evaluated first.

Example 1:

Occurred Time Equals '7/22/2007'

And Username Equal To Sally

Or Username Equal To Harry

And Resource Equal To Line1Computer

In this case, FactoryTalk AssetCentre evaluates first the ANDs and then the OR, so it is as if the expression were written:

(7/22/2007 AND Sally) Or (Harry AND Line1Computer)

Meaning: Include anything Sally did on July 22. Include anything Harry did on the Line1Computer.

Example 2:











Occurred Time Equals '7/22/2007'

And (Username Equal to Sally

Or Username Equal to Harry)

And Resource Equal To Line1Computer

The following table lists the **Conditions** tab's buttons for creating conditions:

Button or graphic	Description
	Create a new condition on which to search. The New Condition dialog box fields and options that appear vary depending on the log data for which you are creating the condition.
 Properties	Change the properties of the selected condition. The Condition Properties dialog box fields and options that appear vary depending on log data for which you are creating the condition.
	Delete the selected condition.
	Place a left parenthesis at the beginning of the selected condition. Use parenthesis to group conditions to control the way the entire expression is evaluated.
	Place a right parenthesis at the end of the selected condition. Use parenthesis to control the way the entire expression is evaluated.
	Place an And in front of the selected condition. By default, each condition has an And in front of it. Use And when you want results to appear in the search results only if both conditions are met.
	Place an Or in front of the selected condition. Use Or when you want an item to appear in the search results if either one or the other condition is met.
	Place a Not in front of the selected condition. Use Not when you want to exclude log records that meet the condition.
	Move a condition higher in the list of shown conditions. While FactoryTalk AssetCentre does evaluate conditions in a specific order (parenthetical conditions before And conditions, and Or conditions last), it does also evaluate those conditions from top to bottom.
	Move Down. Move a condition lower in the list of shown conditions. FactoryTalk AssetCentre evaluates the conditions in the order they appear.

8. When the conditions are created, click **Save (Search Name)**.
9. To quickly see the search results, view the **Preview** tab.

10. To format and modify the recipient list for scheduled search results as well as set the time zone for the computer running the search, complete the **Scheduled Search Operation** tab. For information on completing this tab, click **Help**.

Tip: The **Scheduled Search Operation** tab only appears when you select a scheduled search definition on the **Searches** tab. To add a schedule to an existing search definition, see the online help. Select **Help > Content**. Open the *Searches* chapter and click the **Create or modify a search schedule** topic.

Step 3: Set search security

You can set security for a search definition to determine which users can set security for, save, execute, and delete the search.

Tip: To modify security settings for a search, you must be granted **Configure Security** permission. In addition, you must be granted the **Read** and **Write** permissions. See the steps below.

Do not deny yourself **Read** permission or you will no longer be able to show the **Security Settings for (Search name)** dialog box to change security for the selected search definition. Generally, all FactoryTalk AssetCentre users are initially granted each permission related to search security. To prevent other users from changing your search definition, deny them **Configure Security** permission.

To set search security:

1. Select **View > Searches**, or click the **Searches** button.
2. On the **Searches** tab, select the search for which you want to change security.
3. Select **Edit > Security** (or click the **Security** button at the bottom of the **Searches** tab).
4. Complete the **Security Settings for (Search name)** dialog box. To do this, select the user and then set that user's permissions for the selected search definition, and then click **OK**. To add a user for whom to set security for the selected search definition, at the top of the dialog box, click **Add**.

The **Common** permissions that apply to searches are:

This permission:	Allows the selected user to:
Configure Security	modify the Read, Write, Execute, and Delete settings for this search
Read	show these security settings for the this search
Write	save this search
Execute	run this search
Delete	delete this search

5. Click **OK**.

Step 4: Run searches

To run schedules, you can either activate scheduled searches or manually run a scheduled or unscheduled search. You may want to run a scheduled search manually if you do not want to have to wait for the search's next run time. Running a scheduled search manually does not affect that search's next scheduled run time.

Time Zones

A scheduled search may actually run on a different computer than your client computer. If some computers in your FactoryTalk AssetCentre system are in different time zones, this could confuse the time-related information in your search results. To set the time zone for a computer that is to run a selected scheduled search, see the online help. Select **Help > Contents**. Open the *Searches* chapter and click the **About modifying and saving searches** topic. To set the default time zone for a computer that is to run scheduled searches, click the **Set scheduled search options** topic.

Tip: To run a search, you must be granted **Execute** permission. See [Step 3: Set search security](#) on [page 66](#). To activate and deactivate scheduled searches, you must be granted **Command a Schedule** permission. To run a search immediately, you must be granted the appropriate permission for the type of search you are going to run — **View Audit Log**, **View Event Log**, or **View Diagnostics & Health Log** permission. See [Step 3: Set Feature Security for FactoryTalk AssetCentre](#) on [page 25](#).

Make a search active

To activate scheduled searches so that they run at their next scheduled run time:

1. Select **View > Searches**, or click the **Searches** button.
2. Next to the searches you want to activate, select the **Active** check box. If the selected search is scheduled to run daily at 4:00 P.M., the search will run next at 4:00 P.M. today (or 4:00 P.M. tomorrow if it is already later than 4:00 P.M. today).

Run searches manually

To run a scheduled or unscheduled search immediately:

1. Select **View > Searches**, or click the **Searches** button.
2. On the **Searches** tab, select the search row.
3. Click the **Run Now** button.

Tip: To perform a quick search without complex conditions instead of the full searches described in this manual, see the online help. Select **Help > Contents**. Open the *Logs* chapter and click the **Perform a Quick Search on a log** topic.









Step 5: View and print search results

Once you run a search, the results appear on a separate tab. Use the **Report (Search Name)** tab to view and navigate the results of a search you have run, as well as export and print the search's results.

Tip: To preview a search instead of showing the report, click the **Preview** tab.

To view and print search results:

1. After you run the search, click the **Report (Search Name)** tab.
2. Use the **Report** tab's toolbar to navigate, export, and print the results. The following table lists the **Report** tab's toolbar buttons and provides a brief description of each button's functions.

Button	Description
 Export Report	Export the search results to the desired location on your hard drive. Results are saved in PDF format.
 Print Report	Print the search results. Complete the Print dialog box and click Print .
 Go To First Page	Show the first page of the search results.
 Go To Previous Page	Show the previous page of the search results.
 Go To Next Page	Show the next page of the search results. If the cover page of the report is shown, click this button to see the first page of the report containing the actual search results returned.
 Go To Last Page	Show the last page of the search results.
 Go To Page	Show a specific page of the search results by entering the page number.
 Zoom	Show the search results as larger or smaller using different percentages.

3. To close the **Report** tab, click the **Close** button  on the right side of the tab.

Tip: To learn about additional search tasks (for example, filtering, modifying, renaming, sorting, or deleting searches), refer to the online help. Select **Help > Contents**. Open the *Searches* chapter and then click the desired topic.

Quick Start 5: Open and edit files in Archive

The FactoryTalk AssetCentre Archive is a version control tool that helps manage asset files. Use Archive to keep secure copies of asset configuration files, pin file versions as masters, track versions, and control file use so that only one person at a time can modify a file.

Tip: File size is not limited in **Archive**; file size is only limited by your Microsoft SQL Server's capabilities.

Using Archive, you can:

- **Keep automation files securely archived.** FactoryTalk AssetCentre's Archive uses Microsoft SQL Server to safely store archived files in a relational database. When you store assets in **Archive**, you reduce your need to back up work and prevent accidental deletion of asset data.
- **Ensure that files are modified by one user at a time.** Designate a file you want to work on and ensure no other users can work on the same archived file until your changes are saved in the Archive database.
- **Version files.** **Archive** is similar to a library. To use an archived file, check it out and when you are done, check it in again. As with a library book, only one person can check out a file at a time. The difference is that you can make changes to the checked-out file, so the library keeps a copy of each version of the file. This way, if someone needs to see a version of a file before it was changed, the earlier version can still be obtained. See [Step 2: Check out a file for editing](#) on [page 71](#) and [Step 3: Check in a file](#) on [page 73](#).
- **Keep an existing version available for use while development continues.** Pin the version of a file that you want other users to use. Development can continue on that file and each revision is saved in **Archive**, but if another user gets the file, they get the pinned version. Also, scheduled operations use the pinned version of the master file. For information about pinning files, refer to the online help. Select **Help > Contents**. Open the *Archive* chapter and click the **Pin or unpin files or binders** topic.

Tip: To add files to **Archive**, all you need to do is add assets and their associated files to the asset tree. See [Step 2: Add assets to the asset tree](#) on [page 41](#).

Quick Start steps for managing files in Archive

To work with files in Archive:

- [Step 1: Set a working folder](#) on [page 70](#)
- [Step 2: Check out a file for editing](#) on [page 71](#)
- [Step 3: Check in a file](#) on [page 73](#)
- [Step 4: Get a read-only version of a file](#) on [page 74](#)
- [Step 5: Open a file for viewing](#) on [page 76](#)

Step 1: Set a working folder

To edit a file or binder stored in the Archive database, you must place a copy of the file or binder on your local hard drive. The location on your hard drive is called a **working folder**. Without a working folder, you cannot retrieve files or binders from the Archive database. When you set a working folder for an asset, you set the working folder for all files and binders within the asset.

Types of Working Folders

FactoryTalk AssetCentre has two types of working folders:

- **System working folder.** The location where images of files and binders will be stored when you check out the files for editing or get a read-only version of a file. When the system working folder is set, this working folder applies to all files and binders in an asset, and all FactoryTalk AssetCentre users. For example, if you set a system working folder located at **C:\BOTTLING PLANT** for an asset called **East Conveyor**, when a user gets or checks out the **East Conveyor** asset, the path **C:\BOTTLING PLANT** is created on that user's local computer and will contain all of the **East Conveyor** asset's files. Each asset can only have one system working folder. Any user with Configure System Archive Working folders permission can set a system working folder for an asset.
- **Personal working folder.** The working folder that overrides the system working folder. When you set a personal working folder in Archive, that folder is created on your computer and remains your personal working folder for an asset's files and binders. Other users use the system working folder until they set their own personal working folders. If users set personal working folders for assets on one computer and then launch FactoryTalk AssetCentre on another computer and want to use the same personal working folders, they must set the working folders again.

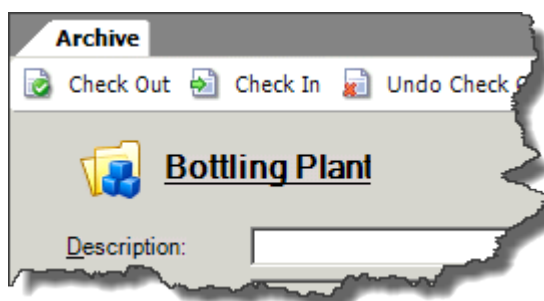
Tip: When you check out, check in, or get a file or binders, you have the option of overriding the current working folder with a temporary location. See [Step 2: Check out a file for editing](#) on [page 71](#), [Step 3: Check in a file](#) on [page 73](#), or [Step 4: Get a read-only version of a file](#) on [page 74](#).

To set a system working folder, you must have **Configure System Archive Working Folders** permission. To set a personal working folder (or to override a working folder when checking in, checking out, or getting a file or binder), you

must have **Configure Personal Archive Working Folders** permission (see [Step 3: Set Feature Security for FactoryTalk AssetCentre](#) on [page 25](#)) and **Set Working Folder** permission for the asset (see [Step 3: Change security settings for an asset](#) on [page 48](#)).

To set a working folder:

1. Select **View > Archive** (or click the **Archive** button).
2. In the asset tree, select the asset containing the files and binders for which you want to set the working folder.
3. On the **Archive** tab, after the **Working folder** field, click **Set**.
4. Complete the **Set Working Folders** dialog box. The current working folder for the selected asset appears at the bottom of this dialog. If you set a personal working folder for yourself, it will override the system working folder. However, all other users will use the system working folder for the asset's files.
5. Click **OK**.
6. To show the contents of a working folder in Windows Explorer, right-click the asset in the asset tree and select **Open Working Folder**. To show the contents of a working folder from within **Archive**, with the asset selected in the asset tree, and click the link at the top of the **Archive** tab:



Step 2: Check out a file for editing

Before modifying any file stored in **Archive**, you must retrieve a copy of the file to the current working folder on your computer. Retrieving a file and making it available for editing is called checking out a file. Only one user at a time can check out a file. If a file is checked out by another user, you must wait until that user checks in the file again before you can check out and edit the file. However, you can get a file that is checked out by another user so that you can view it in your project. For information about getting a read-only version of a file, see [Step 4: Get a read-only version of a file](#) on [page 74](#).

When you check out an asset, you automatically check out all of the files within the asset. You have the option of checking out any files located in subfolders of the asset.

FactoryTalk AssetCentre makes it easy to locate a file you check out by duplicating the asset tree structure in folders and subfolders on your hard drive. A check out duplicates the asset tree structure from the container or folder where you set the working folder to the container or folder where the file you checked out is located.

Tip: To check out files, you must have **CheckOut - CheckIn** permission for the asset. See [Step 3: Change security settings for an asset](#) on [page 48](#).

To check out a file or folder of files:

1. In the asset tree, select the asset containing the file(s) to check out. Once you select an asset in the asset tree, you can also select the file to check out on the **Archive** tab.
2. On the **Archive** tab, click the **Check Out** button.

Tip: You can also right-click an asset in the asset tree (or a file on the **Archive** tab after you select an asset in the asset tree) and select **Check Out**.

3. Complete the **Check out** dialog box by selecting any of the following options:

This option	Performs the following:
Get local copy	Select this option to check out the version of a file from the Archive database and place it in your working folder; any version of the file in your current working folder will be overwritten by the version checked out from the Archive database. Clear this option to preserve the file version in your current working folder. This is useful when you've performed a Get to retrieve a writable version of the file to your current working folder and now want to back up changes you make to that file in Archive . Clearing this option allows you to continue editing the version in your current working folder and back up those changes in Archive the next time you check in the file. For information about getting a version of a file, see Step 4: Get a read-only version of a file on page 74 .
Recursively check out files from subfolders	Normally when you check out an asset, you check out all of the files within the asset. Select this option to also check out all of the files located in subfolders of the asset. This option is only available if you select an asset that contains files in the asset tree.
Override working folders	Select this option to override your current working folder and check out files to a temporary working folder used for this one check out operation only. Type the path of the temporary working folder (you can type the path of a new temporary working folder and the working folder will be created automatically), or click Browse to select the path of the working folder you want to use temporarily. To override the working folder, you must have Configure Personal Archive Working Folders permission (see Step 3: Set Feature Security for FactoryTalk AssetCentre on page 25) and Set Working Folders permission (see Step 3: Change security settings for an asset on page 48).

4. Enter an optional comment to summarize the work. This is helpful when tracking work done in a file. The maximum length for a comment is 2500 characters.
5. Click **OK**. A checkmark appears next to the file link and the check out location of the file appears on the **Archive** tab.

Tip: You can undo a check-out. This reverts a file or an asset's files to the previous version and marks the file as no longer checked out. For information about undoing a check-out, refer to the online help. See **Help > Contents**. Open the *Archive* chapter and click the **Undo a check out** topic.

Step 3: Check in a file

Once edits are completed to a checked-out file, return it to the Archive database. Checking in a file saves a new version so that changes are backed up and protected in the Archive database. When you are working on a file over a long period of time, it is good practice to check in the file daily.

If you check in an asset, you automatically check in all files within the asset. You have the option of checking in any files located in subfolders of the asset as well.

You can only check in a file that someone else has checked out if you have permission.

Tip: To check in files, you must have **CheckOut - CheckIn** permission (see [Step 3: Change security settings for an asset](#) on [page 48](#)). To check in a file someone else has checked out, you must have **Override Archive CheckIn** permission (see [Step 3: Set Feature Security for FactoryTalk AssetCentre](#) on [page 25](#)).

To check in a file or folder of files:

1. In the asset tree, select the file or the asset containing the files to check in.
2. On the **Archive** tab, click the **Check In** button.

Tip: You can also right-click the asset or file in the asset tree (or a file on the **Archive** tab if you select an asset in the asset tree) and select **Check In**.

3. Complete the **Check in** dialog box. The following options are available:

This option:	Performs the following:
Check in and delete the local copy	Check in the file so the changes are backed up in the Archive database, and delete the copy of the modified file from your current working folder.
Check in but keep a local copy	Check in the file so the changes are backed up in the Archive database, and keep a read-only copy of the file in your current working folder. When you check out this file again, you will have to decide whether or not you want to overwrite the file in your working folder. This option is only available when you have Override Removal of Local Copies permission. See Step 3: Set Feature Security for FactoryTalk AssetCentre on page 25 .

Keep checked out	Check in the file so the changes are backed up in the Archive database, but immediately check out the file to yourself again so that you can keep editing it.
Recursively check in files from subfolders	Normally when you check in a device or container, you check in all of the files within that asset. Select this option to also check in any files located in subfolders of the device or container. This option is only available if you select a device or container in the asset tree.
Override check-out location with path	Select this option to check in files from a temporary working folder instead of your current working folder. This is useful if you made a copy of a file and placed it in a location other than the working folder to which you originally checked out the file. To save any changes to the file you copied, click Browse and select the location from which you want to check in the file. To override the working folder, you must have Configure Personal Archive Working Folders permission (see Step 3: Set Feature Security for FactoryTalk AssetCentre on page 25) and Set Working Folders permission (see Step 3: Change security settings for an asset on page 48).

- Enter a comment to summarize the work. This is helpful when tracking work done in a file. The maximum length for a comment is 2500 characters.

Note: Depending on the value assigned to the **Allow Empty Comment at Check In** security setting for a particular user or group, typing a comment may or may not be obligatory upon the check-in.

- Click **OK**. The checkmark is removed from the asset or file on the **Archive** tab. The check-in action, as well as the date and time the file is checked in, appears on the **History** tab. To learn about the **History** tab, see the online help. Select **Help > Contents**. Open the *Archive* chapter and click the **View file history** topic.

Step 4: Get a read-only version of a file

Use **Get** to retrieve a read-only copy of a file or the files in an asset to your current working folder. **Get** allows people who need to use the file (but don't need to edit it) to get the necessary file version. For example, if you want to copy rungs from another ladder program, you can get that program (even if another user has the file checked out), copy the rungs, and then paste them into your file. Getting a file eliminates accidental changes to the master file.

You can get the current version of a file or the files in an asset, or you can select an earlier version. You can also get a file that is marked as checked out, even if you have the file checked out.

FactoryTalk AssetCentre makes it easy to locate a file that you get by duplicating the asset tree structure in folders and subfolders on your hard drive. Getting a file duplicates the asset tree structure from the container or folder where you set the working folder to the container or folder where the file you get is located.

The date and time a file is retrieved appears in the file history. To learn about how Archive sets dates and times for files, see the online help. Select **Help > Contents**. Open the *Archive* chapter and click the **Date and time settings** topic.

Tip: To get read-only versions of files, you must have **Get** permission. See [Step 3: Change security settings for an asset](#) on [page 48](#).

To get the current version of a file:

1. In the asset tree, select the file or asset containing the files to retrieve and click the **Get** button.
2. Complete the **Get** dialog box. The following options are available:

This option:	Performs the following:
Get writable copy	Retrieve an editable instead of read-only copy of the file. This retrieves the most recent or pinned file version into the current working folder.
Recursively get files from subfolders	Place a copy of all files located in subfolders of the selected device, container, or folder into the current working folder. This option is only available when you select a device, container, or folder in the asset tree. It is not available if you select a file.
Overwrite checked-out files	Overwrite any versions of the file in the current working folder with the version you are retrieving from the Archive database.
Override local name	Select this option to provide another name for the file to be placed in the working folder. Select the check box and type a name for the file. When you click OK , the file is placed in the working folder with the specified name.
Override working folders	Select this option to retrieve the file into a temporary working folder, instead of the current working folder, for this Get operation only. Type the exact path of the temporary working folder or click Browse to select the working folder location where you would like to store the retrieved files. To override the working folder, you must have Configure Personal Archive Working Folders permission (see Step 3: Set Feature Security for FactoryTalk AssetCentre on page 25) and Set Working Folders permission (see Step 3: Change security settings for an asset on page 48).

3. Enter an optional comment to summarize the work. This is helpful when tracking work done in a file. The maximum length for a comment is 2500 characters.
4. Click **OK**. The file appears in your current working folder. The **Get** action is shown in the file history unless you select to show version-related activities.

Tip: To get a specific (labeled) version of a file, see the online help. Select **Help > Contents**. Open the *Archive* chapter and click the **Label a file or binder version** and **Get a read-only version of a file or binder** topics.

You can also get a pinned version of a file, if there is one. For more information, see the online help. Select **Help > Contents**. Open the *Archive* chapter and click the **Pin or unpin files or binders** topic.

To learn about additional Archive tasks (for example, promoting, or deleting files from the FactoryTalk AssetCentre Archive), also refer to the online help. Open the *Archive* chapter and click the desired topic.

Step 5: Open a file for viewing

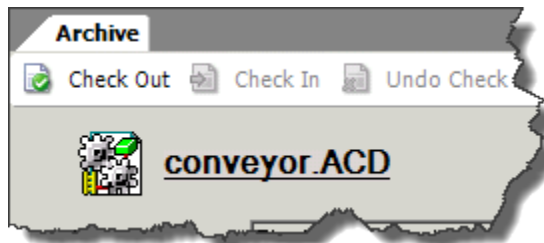
If you have set a working folder for a file, you can choose to open that file to view its contents. This is helpful when you want to make sure you have selected the correct file. Opening a file also allows you to copy its content.

When you open a file and have already placed a local copy of that file in the working folder by either checking out or getting the file, the software program associated with the file opens the file. To set a file association for a file, see the online help. Select **Help > Contents**. Open the *Archive* chapter and click the **Set file associations** topic.

If you do not have a local copy of the file in your working folder when you choose to open the file, FactoryTalk AssetCentre prompts you to either check out the file for editing (see [Step 2: Check out a file for editing](#) on [page 71](#)) or Get a read-only version of the file (see [Step 4: Get a read-only version of a file](#) on [page 74](#)). This allows you to place a local copy of the file in your working folder and have the associated software program open the file at the same time.

To open a file:

1. In the asset tree, right-click the file and select **Open Working Folder**. You can also double-click the file or select it in the asset tree and then at the top of the **Archive** tab, click the file link:



If there is a copy of the file in your working folder, the file's associated software program launches and opens the file.

Tip: If you do not have a working folder set for the file's asset, the message dialog box *Unable to Launch File* appears instead of the **File Retrieval Options** dialog box. See [Step 1: Set a working folder](#) on [page 70](#).
If there is not a copy of the file in your working folder, complete the **File Retrieval Options** dialog box to place the file in your working folder and then either checking out or getting the file. For more information about checking out a file, see [Step 2: Check out a file for editing](#) on [page 71](#). For more information about getting a file, see [Step 4: Get a read-only version of a file](#) on [page 74](#).
If the message *No program is associated with the specified file for this operation*, see [If you cannot open a file](#) on [page 91](#).

2. Close the file when you are done viewing it. Any changes you make to an open file will not be saved unless you check out the file from **Archive**. See [Step 2: Check out a file for editing](#) on [page 71](#).

If the automatic check-in feature is enabled, after done editing the file that checked out from **Archive**, you will be asked if you need to save a new version. For more information on automatic check-in, see the online help. Select **Help > Contents**, and navigate to the **Options dialog box: File Associations** topic.

Quick Start 6: Manage Rockwell Automation hardware life cycle

Assets Lifecycle provides the life-cycle information for Rockwell Automation hardware devices in the system. It shows the life-cycle status in the form of a list that allows you to easily manage the hardware life cycle and make decisions about which device needs upgrade or replacement.

Quick Start steps for managing Rockwell Automation hardware life cycle

To manage the life cycle of Rockwell Automation hardware devices:

- [Step 1: Synchronize life-cycle status](#) on [page 79](#)
- [Step 2: Refresh life-cycle status](#) on [page 80](#)
- [Step 3: View detailed life-cycle status](#) on [page 81](#)

For more information, refer to the online help. Select **Help > Contents**. Open the *Assets Lifecycle* chapter and click the desired topic.

Step 1: Synchronize life-cycle status

Synchronize life-cycle information in the FactoryTalk AssetCentre server and client with the data on the [Rockwell Automation life cycle website](#). You can synchronize the life-cycle information of either assets or asset inventory in the AssetCentre server. The life-cycle synchronization is recommended to run during server null time (time when no scheduled tasks or user interaction is taking place) if possible. With the synchronization process being based on product ID or catalog number quantity, it can take some time to complete based on the total collected, and will require server resources during run time.

Make sure you have an Internet connection for this operation.


To synchronize life-cycle status of assets:

1. Select **View > Assets Lifecycle**, or click the **Assets Lifecycle** button.
2. Click the **Asset** tab.
3. Click **Sync**. A progress bar shows.
4. After the progress, the life-cycle information is updated to the FactoryTalk AssetCentre database and the life-cycle status is updated on the asset list.

To synchronize life-cycle status of asset inventory:

1. Select **View > Assets Lifecycle**, or click the **Assets Lifecycle** button.
2. Click the **Asset Inventory** tab.
3. If you have used an asset inventory file before and don't want to use another version, skip to Step 7.

If this is the first time to use an asset inventory file, the **Asset Inventory** tab is empty. You need to specify an RAAI file. On the right of the **Asset**

Inventory File box, click .

4. On the left of the **Select File** dialog box, select an RAAI file in the asset tree view.
5. On the right of the **Select File** dialog box, select an RAAI file version.
 - Filter by label
Select this option to filter the RAAI files by label.
 - Filter by version
Select this option to filter the RAAI files by version.
 - Latest version
Select this option to use the latest version of the RAAI file.
6. Click **OK**.
7. Click **Sync**. A progress bar shows.
8. After the progress, the life-cycle information is updated to the FactoryTalk AssetCentre database and the life-cycle status is updated on the asset list.

Step 2: Refresh life-cycle status

Refreshing life-cycle information only updates the data on the AssetCentre client with the AssetCentre server. You can refresh the life-cycle information of either assets or asset inventory on the AssetCentre client.

This operation doesn't need an Internet connection.

To refresh life-cycle status of assets or asset inventory:

1. Select **View > Assets Lifecycle**, or click the **Assets Lifecycle** button.
2. To refresh assets, click the **Asset** tab.

To refresh asset inventory, click the **Asset Inventory** tab.

3. Click **Refresh**. A progress bar shows.
4. After the progress, the life-cycle information is updated from the FactoryTalk AssetCentre database to the client and the life-cycle status is updated on the asset list.

Step 3: View detailed life-cycle status

In the asset list on the **Asset** or **Asset Inventory** tab, you can view the detailed life-cycle status of devices, including:

- Product ID: product ID of a device.
- Product Description: product description of a device.
- Lifecycle Status: life-cycle status of a device.
- Discontinued Date: the announced discontinued date.
- Last Update Date: the last time when the life-cycle status was updated.
- Recommended Replacement Product: the recommended product to replace the current one.
- Replacement Category: the nature of the replacement.

To view detailed life-cycle status:

1. Select **View > Assets Lifecycle**, or click the **Assets Lifecycle** button.
2. Click the **Asset** tab or the **Asset Inventory** tab.
3. Click a device in the list. A window of life-cycle information opens.

Tip: For devices in the Active Mature, End of Life or Discontinued status, you can expand the **Replacement Information** to view the recommended replacement product and replacement category.

4. To close the window, click anywhere outside the window.

Tip: If you want to reopen the life-cycle window of an asset you just closed, click another asset then click the one whose life-cycle window you want to open again.

Life-cycle statuses

In the asset list of Assets Lifecycle, there are five statuses appended to each asset, showing their current life-cycle stage.

Status	Description
None	Indicates the life-cycle status is not available for the asset.
Active	Most current offering within a product category.
Active Mature	Product is fully supported, but a newer product or family exists. Gain value by migrating.
End of Life	Discontinued date announced - actively execute migrations and last time buys. Product generally orderable until the discontinued date. ¹

Status	Description
Discontinued	New product no longer manufactured or procured. ² Repair/exchange services may be available.

¹ Outages on specific items may occur prior to the Discontinued date.

² Limited stock may be available in run-out mode, regionally.

Troubleshoot

Troubleshoot the FactoryTalk AssetCentre client

For additional troubleshooting information see the online help.

This section includes the following topics:

- [If the client fails to start](#) on [page 83](#)
- [If the client cannot communicate with the server](#) on [page 84](#)
- [If you cannot enter Design Mode](#) on [page 85](#)
- [If you cannot connect to PanelView Plus devices](#) on [page 85](#)
- [If you cannot connect to MobileView devices](#) on [page 85](#)
- Make sure the client computer is connected to the network and the network is operational.
- Make sure your FactoryTalk AssetCentre server computer is running.
- Make sure the FactoryTalk AssetCentre Server service, IIS and SQL server are all running on the server computer (and the database computer if separate).
- Make sure the correct FactoryTalk Directory is specified. On the machine running the client, select **Start > All Programs > Rockwell Software > FactoryTalk Tools > Specify FactoryTalk Directory Location**.
- If your computer is not authenticated by a domain controller (for example, if it is part of a workgroup instead), turn off the FactoryTalk single sign-in feature. For information about single sign-in, see the FactoryTalk help file. Select **Start > All Programs > Rockwell Software > FactoryTalk Tools > FactoryTalk Help**.
- Make sure the server location setting is correct. On the server computer go to **Start > All Programs > Rockwell Software > FactoryTalk AssetCentre Server > Server Settings**. The server location must be set in this utility, NOT in the FactoryTalk Administration Console.
- Make sure the SQL Connection is set properly. On the server computer go to **Start > All Programs > Rockwell Software > FactoryTalk AssetCentre Server > Data Source Configuration**.
- If the message *The client and server versions are incompatible* appears when you attempt to start the FactoryTalk AssetCentre client, and the

FactoryTalk AssetCentre software installed on the server has been updated, then the software on the client needs to be updated. See the *FactoryTalk AssetCentre Installation Guide* for information on updating the client and agent software.

- If the message *Error initializing FactoryTalk AssetCentre* appears when you attempt to start the FactoryTalk AssetCentre client, your FactoryTalk AssetCentre server may have failed (or you may have lost your network connection to the server) or the client computer may not be part of the FactoryTalk Directory. If you have checked the server (as directed earlier in this list), try adding the client computer to the FactoryTalk Network Directory. From another computer that has access to the FactoryTalk Directory (the FactoryTalk AssetCentre server, for example), use the FactoryTalk Administration Console to add the computer to the FactoryTalk Directory.
- If you are using a firewall, make sure your firewall is configured properly to permit access to the FactoryTalk AssetCentre Server. See the *FactoryTalk AssetCentre Installation Guide* for information on firewall settings.

Tip: For information on port requirements, see the topic **Network requirements** in the *FactoryTalk AssetCentre Installation Guide*. Select **Help > Installation Guide** to open the guide.

If the client cannot communicate with the server

If a client cannot connect to the server (if the server status in the Status Bar is Disconnected) or the client cannot connect to capabilities located on the network (for example, if logs won't show or schedule information does not appear) check the following:

- client computer is connected to the network and the network is operational.
- FactoryTalk AssetCentre Server service, IIS, and SQL Server are all on-line. See below for more information on IIS.
- server location setting is correct. On the server computer select **Start > All Programs > Rockwell Software > FactoryTalk AssetCentre Server > Server Settings**. The server location must be set in this utility, not in the FactoryTalk Administration Console.
- SQL Connection is set properly. On the server computer select **Start > All Programs > Rockwell Software > FactoryTalk AssetCentre Server > Data Source Configuration**.

To make sure IIS is running on the server computer:

1. On supported operating systems (Windows Server 2012 and 2008 R2) of FactoryTalk AssetCentre Server, click **Start**.
2. On the **Start** menu, right-click the **My Computer** icon, and then click **Manage**.

Server Manager appears.

3. In the **Server Manager** tree, expand **Roles**.
4. Under **Roles**, expand **Web Server (IIS)**.
5. Under **Web Server (IIS)**, click **Internet Information Services (IIS) Manager**.
6. In the right pane, under **Connections**, expand the server node.
7. Expand **Sites**, and then click **Default Web Site**.
8. In the right pane, under **Actions**, check if the site is running.

If it is not, start it:

- In the right pane, under **Manage Web Site**, click **Start**.
- You might not have the appropriate permissions to enter Design mode. See [Step 3: Set Feature Security for FactoryTalk AssetCentre](#) on [page 25](#).
- Only one user in your system can be in Design mode at a time. If another user is in Design mode, you will not be able to enter Design mode until that user exits Design mode.
- The server might not be activated. To see if the server is activated, select **Help > About**. Under **Components**, select **FactoryTalk AssetCentre Server Features**, and then below that select **FactoryTalk AssetCentre Server**. Activation information for the server appears on the right.

If the server needs to be activated, on the **About** dialog box, click **Refresh**. If the server is still not activated, see the FactoryTalk Activation Manager online help for more information.

- The server, database, or FactoryTalk Directory may be offline or unavailable.

If you cannot enter Design Mode

If you cannot connect to PanelView Plus devices

FactoryTalk Linx, formerly known as RSLinx Enterprise, must be installed on the client computer to communicate with PanelView Plus operator interfaces. See the *FactoryTalk AssetCentre Installation Guide* for information on installing FactoryTalk Linx.

FactoryTalk View ME must be installed on the agent computer to communicate with PanelView Plus operator interfaces. This is a separate installation that is not included as part of the FactoryTalk AssetCentre installation.

If you cannot connect to MobileView devices

FactoryTalk Linx, formerly known as RSLinx Enterprise, must be installed on the client computer to communicate with MobileView operator interfaces. FactoryTalk Linx must be version 5.71 or higher. See the *FactoryTalk AssetCentre*

Installation Guide for information on installing FactoryTalk Linx.

FactoryTalk View ME must be installed on the agent computer to communicate with MobileView operator interfaces. This is a separate installation that is not included as part of the FactoryTalk AssetCentre installation.

Troubleshoot Schedules

This section includes the following topics:

- [If a schedule did not run](#) on [page 86](#)
- [If a schedule no longer appears on the Schedules tab](#) on [page 86](#)
- [If an asset is missing from a schedule](#) on [page 86](#)
- [My schedule contains extra devices that I don't want in the schedule](#) on [page 87](#)
- [If you are prompted to install agents when creating a Disaster Recovery schedule](#) on [page 88](#)
- [If you see the message "Failed to create RSLogix 5 \[or 500\] data \[or program ladder\] file list"](#) on [page 88](#)
- [If the scheduled Disaster Recovery operation never completes](#) on [page 89](#)

If a schedule did not run

You must make a schedule active for its status to be Waiting to Run or Running. See [Step 3: Run schedules](#) on [page 57](#).

If a schedule no longer appears on the Schedules tab

Any user with **Delete a schedule** permission can delete any schedule from FactoryTalk AssetCentre. You do not have to create a schedule to be able to delete that schedule. If you or another FactoryTalk AssetCentre user has permission and deletes an asset from the asset tree, the schedule will be deleted. This occurs if an asset is the starting point (the top level asset) of a schedule. The schedule cannot be retrieved. You must add the device to the asset tree again and then recreate the asset's schedule. For more information about deleting assets, see the online help. Select **Help > Contents**. Open the *Assets* chapter and click the **Delete an asset** topic.

If an asset is missing from a schedule

If you or another FactoryTalk AssetCentre user deletes an asset from the asset tree, that asset will be removed from any schedules in which it was included. To restore that asset to the schedule, you would have to add the asset back into the container in the asset tree that is the starting point of the schedule. When you add the asset back to the container, it will appear in the schedule again, but it will have the default operation properties set under **Tools > Options**. If these are not the desired properties, you can change the properties for that asset in that schedule. See the online help. Select **Help > Contents**. Open the *Schedules* chapter and click the **Modify scheduled operation properties** topic.

My schedule contains extra devices that I don't want in the schedule

Devices meeting the necessary criteria will automatically be added to a scheduled container as soon the device is added to the container in the asset tree. To exclude assets from a schedule, disable the assets you do not want to include in the schedule. See the online help. Select **Help > Contents**. Open the *Schedules* chapter and click the **Enable or disable scheduled assets** topic.

If a scheduled operation fails

- Certain operations, such as Backup and Compare, may fail if the operation requires that a device has a master file and it does not. To select which version of the file in **Archive** will serve as the master file to the device, see the online help. Select **Help > Contents**. Open the *Assets* chapter and click the **Add an asset** topic.
- The RSLinx path on the client computer where the device's addressing information was set may not match the RSLinx path on the agent computer running the schedule. All computers in the FactoryTalk AssetCentre system must have the same RSLinx drivers and paths.
- Scheduled events for Rockwell Automation Logix 5000 processors will fail if FactoryTalk Security is enabled for that devices' programming software (RSLogix 5000 versions 16 and earlier). The problem is fixed in RSLogix 5000 versions higher than 16. For RSLogix 5000 versions 16 and earlier, running scheduled events requires single sign-on for these versions. This issue does not affect other device's schedules (such as robots or PanelView devices). If a schedule contains both Logix 5000 processors and other devices, the scheduled event will only fail for those Logix 5000 processors for which FactoryTalk Security is enabled in the programming software; the event will complete for the other devices.

To configure the system so that scheduled operations will succeed even with security enabled in the RSLogix software, see the online help. Select **Help > Contents**. Open the *Welcome to FactoryTalk AssetCentre* chapter and click the **About the configuration for security-enabled RSLogix products** topic.

You will be unable to create a schedule for an asset that is to be the starting point of a schedule if the asset isn't supported by the scheduled operation. Also, a schedule will not include an asset that is not supported by the selected operation. For example, if you have Disaster Recovery for Rockwell devices, but did not purchase Disaster Recovery for Motoman Robots, you won't be able to create a schedule for a Motoman robot, nor will a Motoman robot appear in a schedule for its parent container.

If you are prompted to install agents when creating a Disaster Recovery schedule

An agent is a program capability (such as Disaster Recovery) that can be located and run on a computer to help another computer complete a task. Agents or operations allow work to be distributed and shared among multiple computers to spread processing load and speed up operations. When a server needs an agent to perform a task, it locates the computer running the operation and assigns the task to that agent. The agent then reports the task's completion to the server.

If you receive a message to install agents or that no agents are installed, the software cannot contact any agents (for example, *Unable to create a new schedule ... No licensed agents are available*). The computers running the agents are not currently available on the network, the agent software needs to be updated, or there are no computers with agents installed on the network.

- When you create a Disaster Recovery schedule, make sure you have not selected an invalid asset, such as a binder or a file. You cannot create any schedules on a binder or file.
- Make sure you have selected a device asset for which you have the Disaster Recovery capability. The Disaster Recovery capability operates only on device assets for which you have purchased the Disaster Recovery capability. You can get Disaster Recovery activation for Rockwell Automation devices, for FANUC robots, and for Motoman robots. See the *FactoryTalk AssetCentre Installation Guide*.
- Creating a Disaster Recovery schedule requires that at least one computer on your network has the Disaster Recovery agent installed on it. If there are no computers with the agent software installed, install the agent software. See the topic "Install FactoryTalk AssetCentre agents" in the *FactoryTalk AssetCentre Installation Guide*.
- If the agent is installed, make sure the computers on which the agent is installed are running and available on your network and that the Disaster Recovery capability is activated. See the *FactoryTalk AssetCentre Installation Guide*.
- The agent software must be the same version as the server. To update the agent software, see the topic "Install FactoryTalk AssetCentre agents" in the *FactoryTalk AssetCentre Installation Guide*.

If you see the message "Failed to create RSLogix 5 [or 500] data [or program ladder] file list"

This message appears if you do not have the RSLogix 5 or RSLogix 500 programming software installed on the client computer on which you are specifying which files and data will be compared during a Backup and Compare operation. Install the appropriate RSLogix programming software on the client computer or use a client computer that already has the programming software.

If the scheduled Disaster Recovery operation never completes

The agent that actually performs the operation may be busy, unavailable, or uninstalled. If *Waiting for Interface* appears next to the scheduled assets in the lower left pane of the **Schedules** tab and it never changes, then either all agents are busy or no agents are online. You can check all schedules on the **Schedules** tab to see whether any are running (and thus using the available agent or agents). You can also check the status bar to see how many agent computers are connected to the system.

If all agents are online, you may need to install the Disaster Recovery agent on more computers or change the execution times so schedules are not running at the same time. To do this, see the topic "Install FactoryTalk AssetCentre agents" in the *FactoryTalk AssetCentre Installation Guide*.

Another reason can be that the FactoryTalk AssetCentre server has been updated, but the software on the agent computer has not been updated. If the agent software version is not compatible with the server software, the agent will not run. A message is logged in the System Event log and the AssetCentre Event log. You can also see the number of active agents appears in the status bar of the FactoryTalk AssetCentre client. To update the agent software, see "Install FactoryTalk AssetCentre agents" in the *FactoryTalk AssetCentre Installation Guide*.

Troubleshoot e-mail notifications

If e-mail notifications do not reach their recipients

This section includes the following topic:

- [If e-mail notifications do not reach their recipients](#) on [page 89](#)
- Make sure you are using valid e-mail addresses. E-mail addresses must be in standard SMTP format (for example, myaddress@domain.com). Other types of e-mail addresses are not handled by FactoryTalk AssetCentre.
- Check the Event log to make sure the scheduled operation is completing. See [Step 1: View Logs](#) on [page 60](#).
- Check your schedule definitions on the **Schedules** tab to make sure there are e-mail addresses assigned to receive notifications. See [Step 2: Set up recipient lists for schedule results](#) on [page 55](#).
- Make sure the FactoryTalk AssetCentre server is set up to send e-mail. To do this, log onto the FactoryTalk AssetCentre server computer, and then select **Start > Programs > Rockwell Software > FactoryTalk AssetCentre Server > Server Settings**. Consult with your e-mail administrator for the correct settings.
- If you are using a firewall (such as the Windows Firewall), make sure the ports used to send e-mail traffic are open. Also make sure that SMTP services are permitted to send traffic through your firewall.

Troubleshoot Logs

This section includes the following topics:

- [If you cannot view a log on page 90](#)
- [If no data appears in a log on page 90](#)
- [If you cannot refresh a log on page 90](#)
- [If you cannot show a previously viewed log on page 90](#)

If you cannot view a log

- You might not have the appropriate permissions to view the specific log. See [Step 3: Set Feature Security for FactoryTalk AssetCentre on page 25](#).
- Your server may not be activated. To see if the server is activated, select **Help > About**. Under **Components**, select **FactoryTalk AssetCentre Server Features** and then in the left pane, select **FactoryTalk AssetCentre Server**. Activation information on the server appears on the right.

If the server needs to be activated, on the **About** dialog box, click **Refresh**. If the server is still not activated, refer to the FactoryTalk Activation Manager online help and contact your system administrator.

If no data appears in a log

- **All logs.** If no data appears in a log, you may not have permission to view the log. See [Step 3: Set Feature Security for FactoryTalk AssetCentre on page 25](#). There might also be an error regarding your connection to the server. See [If the client cannot communicate with the server on page 84](#).
- **Diagnostics and Health Log.** Initially, only previously existing data appears in the Diagnostics and Health Log if that data was imported from the RSMACC Network Health Solution. This data is not updated by FactoryTalk AssetCentre.

New data is logged in the Diagnostics and Health Log only if RSNetWorx MD is installed on your system. Contact your system administrator.

If you cannot refresh a log

If you try and refresh the data in the currently shown log and the message *You do not have permission to view the selected log* appears, your permission to view the log was removed after you shown the log. See [Step 3: Set Feature Security for FactoryTalk AssetCentre on page 25](#).

If you cannot show a previously viewed log

If you try and show a log which you could view previously and the message *You do not have permission to view the selected log* appears, your permission to view the log was removed since you last viewed the log. See [Step 3: Set Feature Security for FactoryTalk AssetCentre on page 25](#).

Troubleshoot Archive

This section includes the following topics:

- [If you cannot check in a file on page 91](#)
- [If you cannot open a file on page 91](#)
- [If the wrong program opens a file on page 91](#)
- [If a button is not available on page 91](#)

- [If you performed a recursive check out and the subfolders didn't copy](#) on [page 91](#)

If you cannot check in a file

You may have changed an asset's working folder since checking out the file. Make sure that the working folder points to the correct location of the checked-out file. See [Step 1: Set a working folder](#) on [page 70](#).

If you cannot open a file

Before opening a file, you must retrieve an image of the file to the current working folder or you will be prompted to either get a read-only copy of the file or check out the file for editing. See [Step 5: Open a file for viewing](#) on [page 76](#). If the message *No program associated with the specified file for this operation* appears, you need to specify the software program that should open the file. See the online help. Select **Help > Contents**. Open the *Archive* chapter and click the **Set file associations** topic.

If the wrong program opens a file

FactoryTalk AssetCentre allows you to set file associations to determine the software product that opens a file. The wrong file association may be set for a file type. See the online help. Select **Help > Contents**. Open the *Archive* chapter and click the **Set file associations** topic.

If a button is not available

If a button or field on the **Archive** tab is disabled, it generally means the operation cannot be performed because the user doesn't have the required permission. See [Step 3: Set Feature Security for FactoryTalk AssetCentre](#) on [page 25](#). Also, the asset state may not permit the operation. For example, you cannot check in a file that has not been checked out.

If you performed a recursive check out and the subfolders didn't copy

If an asset's subfolder has its own working folder specified, files will be copied to that working folder rather than the working folder of the asset. See [Step 1: Set a working folder](#) on [page 70](#).

Legal Notices

Copyright notice

Copyright © 2018 Rockwell Automation Technologies, Inc. All Rights Reserved.
Printed in USA.

This document and any accompanying Rockwell Software products are copyrighted by Rockwell Automation Technologies, Inc. Any reproduction and/or distribution without prior written consent from Rockwell Automation Technologies, Inc. is strictly prohibited. Please refer to the license agreement for details.

End User License Agreement (EULA)

You can view the Rockwell Automation End-User License Agreement ("EULA") by opening the License.rtf file located in your product's install folder on your hard drive.

Other Licenses

This is a product of Rockwell Automation and contains HCF SDC-625 technology. The HCF SDC-625 technology is owned by Hart Communication Foundation (HCF), 9390 Research Blvd., Suite i-350 Austin, Texas 78759, and may not be adopted, copied, reproduced, modified, licensed, sub-licensed, sold or resold other than under license from HCF.

Trademark Notices

Allen-Bradley, Arena, ControlLogix, Data Highway Plus, DH+, Data Highway II, Datapac, Emonitor, Enlab, Enlube, Enpac, Enshare, Entek, Entrx, Enwatch, eProcedure, FactoryTalk, GuardLogix, GuardPLC, Linx, Logix5000, MicroLogix, MobileView, MobileView Guard, MotorMonitor, PanelBuilder, PanelView, PhaseManager, PlantLink, PLC-2, PLC-3, PLC-5, Powermonitor, ProcessLogix, Propack Data, Rockwell, Rockwell Automation, Rockwell Software, RSAssetSecurity, RSBizWare, RSBizWare BatchCampaign, RSBizWare BatchHistorian, RSBizWare Coordinator, RSBizWare Historian, RSBizWare MaterialTrack, RSBizWare PlantMetrics, RSBizWare Scheduler, RSBizWare Tracker, RSEnergyMetrix, RSLinx, RSLogix, RSLoop Optimizer., RSNetWorx, RSNetWorx for ControlNet, RSNetWorx for DeviceNet, RS PMX, RSPower, RSSql, RSTune, RSVIEW, RSVIEW Administration Console, SIMAN, SLC, SoftLogix, Studio 5000, VersaView, WINtelligent, and XM are trademarks of Rockwell Automation, Inc.

Any Rockwell Automation software or hardware not mentioned here is also a trademark, registered or otherwise, of Rockwell Automation, Inc.

Other Trademarks

Microsoft, Microsoft Access, SQL Server, Windows, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, Windows 10, Windows 8.1, and Windows 7 are either registered trademarks or trademarks of Microsoft Corporation in the United States and other countries.

Adobe, Acrobat, and Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and other countries.

Android™ is a registered trademark of Google Inc.

IOS is either a registered trademark or trademark of Cisco in the United States and other countries.

iPad and iPhone are registered trademarks of Apple Inc.

Samsung, Galaxy, and Galaxy Tab S are registered trademarks of Samsung Electronics Co., Ltd.

Oracle is a registered trademark of Oracle Corporation.

ControlNet is a registered trademark of ControlNet International.

DeviceNet is a trademark of the Open DeviceNet Vendor Association, Inc. (ODVA).

Ethernet is a registered trademark of Digital Equipment Corporation, Intel, and Xerox Corporation.

OLE for Process Control (OPC) is a registered trademark of the OPC Foundation.

All other trademarks are the property of their respective holders and are hereby acknowledged.

Warranty

This product is warranted in accordance with the product license. The product's performance may be affected by system configuration, the application being performed, operator control, maintenance, and other related factors. Rockwell Automation is not responsible for these intervening factors. The instructions in this document do not cover all the details or variations in the equipment, procedure, or process described, nor do they provide directions for meeting every possible contingency during installation, operation, or maintenance. This product's implementation may vary among users.

This document is current as of the time of release of the product; however, the accompanying software may have changed since the release. Rockwell Automation, Inc. reserves the right to change any information contained in this document or the software at any time without prior notice. It is your responsibility to obtain the most current information available from Rockwell when installing or using this product.

Environmental compliance

Rockwell Automation maintains current product environmental information on its website at

<http://www.rockwellautomation.com/rockwellautomation/about-us/sustainability-ethics/product-environmental-compliance.page>

Contact Rockwell Automation

Customer Support Telephone — 1.440.646.3434

Online Support — <http://www.rockwellautomation.com/support/>

A

Actions

- allow 50
- deny 50
- permissions 50

Activate 7

- Disaster Recovery 53
- FactoryTalk AssetCentre server 93
- servers 93

Add

- Address Book contacts to groups 28
- client computers 24
- users 24

Address Book 28

Addressing info 43

Agents

- definition 91
- install 92
- not complete operation 92
- prompted to install 91

Archive 43

- button not available 95
- cannot check in a file 94
- cannot open a file 94
- check in and delete local copy 77
- check out files 73
- Date and time settings 79
- delete files 79
- file associations 80
- File size 73
- get local copy 77
- get read-only file version 79
- keep checked out 77
- label files 79
- open files 80
- override check out location with path 77
- override working folders 75
- pin files 79
- promote 79
- set working folders 74
- subfolders not copied in recursive check out 95
- troubleshoot 94
- version control 73

Archive button 18

Asset Catalog

device types 13

position 13

Asset tree 13

- add assets 43
- Design 41
- flow of materials 41
- machine type 41
- order of assets 41
- physical location 41

Asset View 12

Assets

- add to asset tree 43
- change security settings for 50
- Containers 13
- definition 12
- devices 13, 43
- do not appear in container schedule 91
- exclude from schedule 91
- files, folders and generic containers 43
- Link 74
- miss from schedules 90
- move affects on schedules 60
- order of 41
- permission to add to or show in asset tree 50
- process devices 13
- roots 43
- security inheritance 43
- types 14

Assets button 18

Associate files 80

Audit Log

- search 64
- view 61, 62

B

Back up 53

Backup and Compare reports 57

C

Calibration button 18

Calibration Management capability 7, 18

Check in 77

- delete local copy 77
- files in subfolders 77

- keep checked out 77
- keep local copy 77
- override check out location with path 77
- Check out 75
 - files for editing 75
 - override working folders 77
 - recursively 95
- Children 50
- Client
 - add 24
 - cannot communicate with server 88
 - configure 23
 - Elements 11
 - fails to start 87
 - Navigate 11
 - run 11
- Compare files 53
- Compare Report file 58
- Completion e-mail lists 58
- Computers 24
- Configuration data files 43, 53, 56
- Connection Status 88
- Contact Technical Support 8
- Containers 13
 - devices do not appear as asset in schedules 91
- Copy button 18
- Create 64
- Create a new schedule permission 26
- Create a Search permission 26
- Cut button 18

D

- Date and time settings 79
- Delete button 18
- Design 41
- Design mode 12
 - cannot enter 89
- Device
 - activate 53
 - Addressing info 43
 - assets 13, 43
 - configuration data 43
 - files 43, 53
 - process devices 13
 - schedule 53
 - types 13

- Diagnostics & Health Log
 - populate with data 61
 - search 64
 - view 61, 62
- Disaster Recovery 53
 - operations and schedules 56
- Disconnected status 88

E

- Edit Address Book permission 26
- Edit files 73, 75, 80
- Elements 11
- E-mail
 - existing addresses 28
 - SMTP format 93
 - troubleshoot notifications 93
- End of Schedule reports 57
 - send 58
- Equipment assets 13
- Error messages
 - Error while updating application files 87
 - Failed to create RSLogix 5 or 500 data or program ladder file list 92
 - prompt to install agents when creating Disaster Recovery schedules 91
 - The client and server versions are incompatible 87
 - Unable to create a new schedule ... No licensed agents are available 91
 - You do not have permission to view the selected log 94
- Event Log
 - search 64
 - view 61, 62
- Export Report button 70

F

- FactoryTalk AssetCentre client
 - Elements 11
 - fails to start 87
 - Navigate 11
 - run 11
 - troubleshoot 87
- FactoryTalk AssetCentre server 93
 - communication error 88
 - connection status 20, 88
- FactoryTalk Linx 89
- FactoryTalk View ME 89
- Feature security 26
- File assets 13, 43

File size 73

Files

- associate with devices 43
- associations 80
- Back up 53
- cannot check in a file 94
- Check in 77
- Check out 75
- Compare files 53
- Compare Report file 58
- Configuration data files 43, 53, 56
- delete files 79
- devices 43, 53
- Edit files 73, 75, 80
- get files from subfolders 79
- Get local copy 75
- get writable copy 79
- keep checked out 77
- label files 79
- master 53
- open files 80
- override check out location with path 77
- override working folders 79
- overwrite checked-out 79
- pin files 79
- promote 79
- secure 73

Firewalls 87, 93

Folder assets 13, 43

Folders

- Check in 77
- Check out 75

G

Generic container assets 13, 43

Get local copy 75

Go to

- First Page button 70
- Last Page button 70
- Next Page button 70
- Page button 70
- Previous Page button 70

Group

- Address Book contacts to groups 28
- Computers 24
- users 24

I

Install agents 91, 92

Instrument assets 13

L

Link 74

Logs

- cannot refresh 94
- cannot show 94
- cannot view 93
- no data 94
- search 61
- troubleshoot 93
- view 61, 62

Logs button 18

Loop assets 13

M

Make active schedules 56, 59, 69

Manually running schedules 70

Master files

- Backup and Compare 53
- definition 53
- scheduled operation failure 91

Menu bar 18, 70

Microsoft SQL Server 73, 88

N

Navigate 11

New button 18

O

Open 80

Operations

- Disaster Recovery 56
- fail 91

Organizational assets 13

Overload 92

Override

- check out location with path 77
- override working folders 75

P

- PanelView Plus devices 89
- Paste button 18
- Permissions
 - actions 50
 - configure search settings 68
 - Create a new schedule 26
 - Create a Search 26
 - Edit Address book 26
 - run searches 68
 - show search security settings 68
 - Switch to Design mode 26
 - View a schedule 26
 - View Address Book 26
 - View Audit Log 26
 - View Diagnostics and Health Log 26
 - View Event Log 26
 - view log 94
- Personal working folders 74
- Pinning files 79
- Policy 26
 - definitions 27
- Preview
 - search 64
 - search results 70
- Print button 18
- Print Report button 70
- Process device assets 13
- Properties button 18

Q

- Quick Search 61, 70

R

- Read-only file versions 79
- Recipients 57
- Recurrence patterns 56, 64
- Recursively check out 95
- Reports 57
- Results 57
- Right-click menus 20
- Root assets 43
- RSLinx Enterprise 89
- Run

- clients 11
- schedules 59, 60
- searches 69

S

- Save button 18
- Schedule results 57
- Schedules 53, 64
 - assets missing 90
 - changes when assets are moved 70
 - Disaster Recovery 56
 - does not appear on Schedules tab 90
 - e-mail recipients 56
 - excludes assets 91
 - fail 91
 - impact from time zones 69
 - make active 56, 59, 69
 - name 56
 - Recurrence patterns 56, 64
 - Results 57
 - run 59
 - run manually 60, 70
 - run times 56
 - troubleshoot 90
- Schedules button 18
- Search 61, 64
 - conditions 64
 - Create 64
 - criteria 64
 - format 64
 - preview 64
 - recipient e-mail lists 64
 - run 69
 - schedule and unschedule 61
 - security 68
 - show 64
- Search results 70
- Searches button 18
- Secure files 73
- Security
 - actions 50
 - add assets to asset tree 50
 - change for assets 50
 - Children 50
 - configure search settings 68
 - Feature security 26

- inheritance 43
- list children 50
- Policy 26
- run searches 68
- show search security settings 68
- Send
 - Backup and Compare reports 58
 - Backup reports 58
 - End of Schedule reports 58
- Server 88
 - activate 93
 - connection status 20, 88
 - FactoryTalk AssetCentre communication error 88
 - Microsoft SQL Server 73, 88
 - Show Help button 18
- site binding
 - configure 33
- Source control 43
- SSL certificate
 - add authority 33
 - create 31
 - import 32
- SSL protocol
 - configure 31, 33, 34
- Status
 - Disconnected status 88
 - FactoryTalk AssetCentre server connection 20, 88
- Status Bar 20
- Subfolders
 - recursively check in files 77
 - recursively check out files 75
- Switch to Design mode 26
- System assets 13
- System working folders 74

T

- Tasks 26
- Test instrument assets 13
- Time zones 69
- Toolbar 18
- Troubleshoot
 - Archive 94
 - Design mode 89
 - e-mail notifications 93
 - FactoryTalk AssetCentre client 87
 - logs 93

- PanelView Plus 89
- schedules 90

U

- Unscheduled searches 64
- Upload master file 53
- Users
 - add 24
 - deny tasks 26
 - group 24

V

- Version control 43, 73
- View 61, 62

W

- Web Client
 - access 21
 - definition 21
- Windows Authentication
 - configure 36
 - turn on 37
- Working folders
 - override on get 79
 - override working folders 77
 - Personal working folders 74
 - set working folders 74
 - System working folders 74
 - temporary 77
 - types of 74
- Workspace Pane 17

Z

- Zoom button 70

Rockwell Automation support

Rockwell Automation provides technical information on the web to assist you in using its products. At <http://www.rockwellautomation.com/support> you can find technical and application notes, sample code, and links to software service packs. You can also visit our Support Center at <https://rockwellautomation.custhelp.com> for software updates, support chats and forums, technical information, FAQs, and to sign up for product notification updates.

In addition, we offer multiple support programs for installation, configuration, and troubleshooting. For more information, contact your local distributor or Rockwell Automation representative, or visit <http://www.rockwellautomation.com/services/online-phone>.

Installation assistance

If you experience a problem within the first 24 hours of installation, review the information that is contained in this manual. You can contact Customer Support for initial help in getting your product up and running.

United States or Canada	1.440.646.3434
Outside United States or Canada	Use the Worldwide Locator available at http://www.rockwellautomation.com/locations , or contact your local Rockwell Automation representative.

New product satisfaction return

Rockwell Automation tests all of its products to ensure that they are fully operational when shipped from the manufacturing facility. However, if your product is not functioning and needs to be returned, follow these procedures.

United States	Contact your distributor. You must provide a Customer Support case number (call the phone number above to obtain one) to your distributor to complete the return process.
Outside United States	Please contact your local Rockwell Automation representative for the return procedure.

Documentation feedback

Your comments will help us serve your documentation needs better. If you have any suggestions on how to improve this document, complete the feedback form, publication [RA-DU002](#).



Rockwell Otomasyon Ticaret A.Ş., Kar Plaza İş Merkezi E Blok Kat:6 34752 İçerenköy, İstanbul, Tel: +90 (216) 5698400

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

Americas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
Europe/Middle East/Africa: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
Asia Pacific: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Rockwell Automation Publication - FTAC-GR002D-EN-E - February 2018

	DESIGN, SUPPLY, INSTALLATION, TESTING & COMMISSIONING OF LOCAL SCADA SYSTEM ALONG WITH NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX		
PO: 3761700080	DEWA Doc No.: RFX72-DES-FDS	Contractor Doc No: PRJ212-CMN-INS-FDS-0001	Date: 29-Jul-2018
RFX - 2131600072	FUNCTIONAL DESIGN SPECIFICATION (FDS)		Rev: 1 Attachment-3

ATTACHMENT 3 – CONTROL ROOM LAYOUT AND PANEL GENERAL ARRANGEMENT

SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX

PHASE-3 LAYOUT DRAWING
(PRIMARY CONTROL CENTER)

PRJ212-PH3-INS-LAY-0001-01

REFERENCE DRAWINGS/DOCUMENTS:								<div><div><div>هيئة كهرباء ومياه دبي</div><div>Dubai Electricity & Water Authority</div></div><div><div></div><div></div></div></div> <div>P.O. BOX: 564, DUBAI, UAE. TEL: 00971-4-324 4444. FAX: 00971-4-324 4922</div>	CLIENT	<div><div><div>DEWA PRJ REF : RFX-2131600072</div><div>DEWA PO REF : PO: 3761700080</div></div><div><div>DEWA DWG. NO.</div><div>RFX72-SRV-LAY3</div></div></div>	<div><div><div><div></div><div>Silvertech</div></div><div><div>P.O. BOX: 17910, JEBEL ALI, DUBAI, U.A.E</div><div>T: +971 (4) 8995000, F: +971 (4) 8995001</div><div>www.silvertech-me.com</div></div></div></div>		SCALE: N.T.S.
	3	02.07.18	RE-ISSUED FOR APPROVAL	SAA	PLP	NH	AA				SIZE: A3		
	2	17.05.18	RE-ISSUED FOR APPROVAL	SJM	JLK	NH	AA						
	1	16.01.18	ISSUED FOR APPROVAL	SAA	JLK	NH	AA		PROJECT:				
	0	17.12.17	ISSUED FOR REVIEW	SAA	JLK	NH	AA		SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA	STME DWG. NO.	SHEET	REV.	
	ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD		SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX - PHASE-3 LAYOUT DRAWING	PRJ212-PH3-INS-LAY-0001	01 OF 03	3	

PRJ212-PH3-INS-LAY-0001-02

SHEET NO.	DESCRIPTION	FILE NAME	DATE	REVISIONS				PURPOSE OF ISSUE
				0	1	2	3	
1	PHASE-3 LAYOUT DRAWING - COVER SHEET	PRJ212-PH3-INS-LAY-0001-01	02.07.18	X	X	X	X	RE-ISSUED FOR APPROVAL
2	PHASE-3 LAYOUT DRAWING - INDEX SHEET	PRJ212-PH3-INS-LAY-0001-02	02.07.18	X	X	X	X	RE-ISSUED FOR APPROVAL
3	PHASE-3 LAYOUT DRAWING	PRJ212-PH3-INS-LAY-0001-03	02.07.18	X	X	X	X	RE-ISSUED FOR APPROVAL
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								
17								
18								
19								
20								
21								
22								
23								
24								
25								
26								
27								
28								
29								
30								
31								
32								
33								
34								
35								
36								
37								
38								

REFERENCE DRAWINGS/DOCUMENTS:

3	02.07.18	RE-ISSUED FOR APPROVAL	SAA	PLP	NH	AA	
2	17.05.18	RE-ISSUED FOR APPROVAL	SJM	JLK	NH	AA	
1	16.01.18	ISSUED FOR APPROVAL	SAA	JLK	NH	AA	
0	17.12.17	ISSUED FOR REVIEW	SAA	JLK	NH	AA	
ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD	

CLIENT

هيئة كهرباء ومياه دبي

Dubai Electricity & Water Authority




P.O. BOX: 564, DUBAI, UAE. TEL: 00971-4-324 4444. FAX: 00971-4-324 4922

DEWA PRJ REF : RFX-2131600072
DEWA PO REF : PO: 3761700080
DEWA DWG. NO.
RFX72-SRV-LAY3

PROJECT:
SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA
SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY
IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX - PHASE-3 LAYOUT DRAWING

VENDOR



Silvertech

إدارة مشاريع المياه والكهرباء

P.O. BOX: 17910, JEBEL ALI, DUBAI, U.A.E.
T: +971 (4) 8995000, F: +971 (4) 8995001
www.silvertech-me.com

SCALE:
N.T.S.

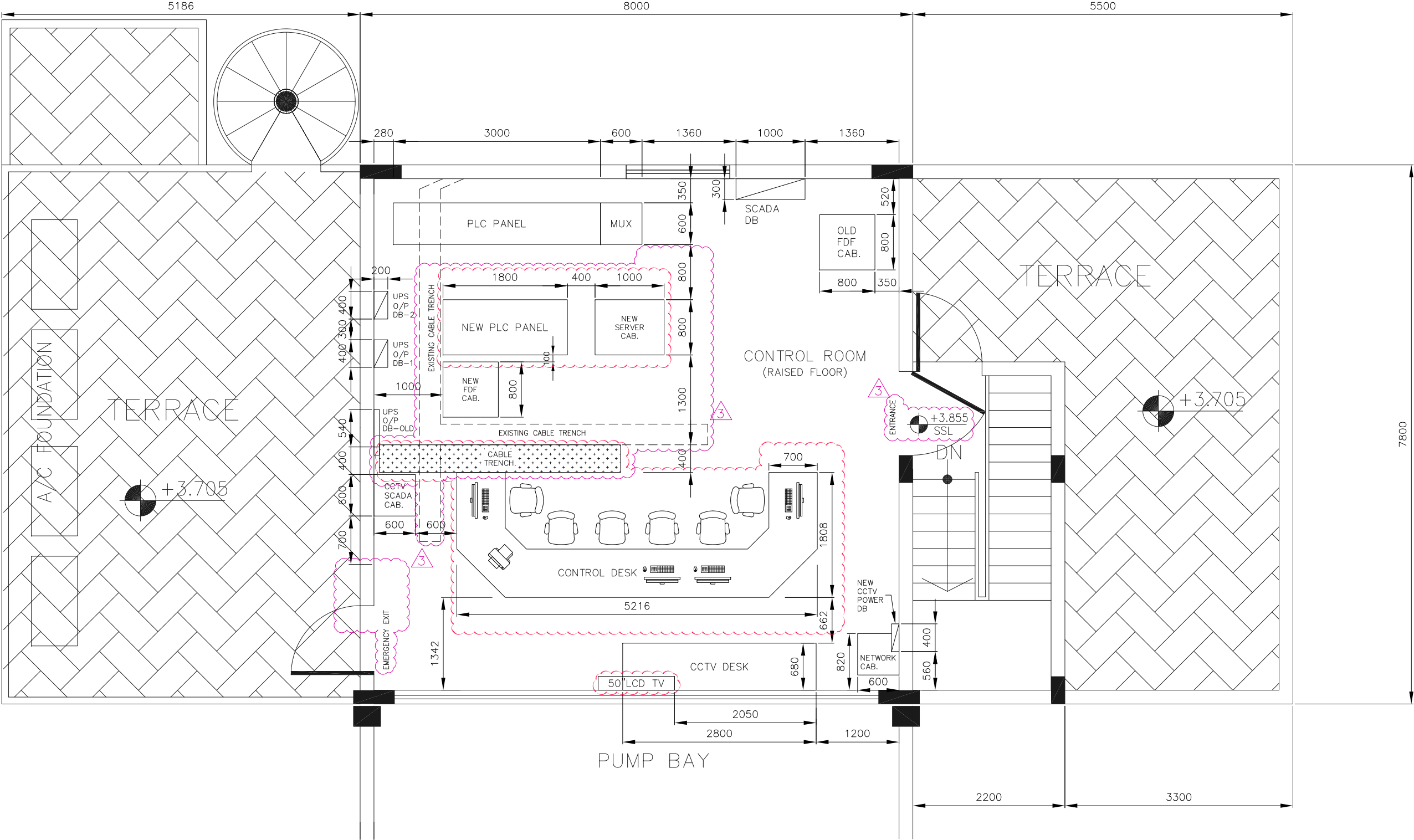
SIZE:
A3

REV.
3

STME DWG. NO.
PRJ212-PH3-INS-LAY-0001

SHEET
02 OF 03

PRIMARY CONTROL CENTER



EXISTING NAJMA PUMPING STATION 3 CONTROL ROOM (1F)


PRJ212-PH3-INS-LAY-0001-03

LEGEND:-

- SCOPE OF WORK UNDER THIS PROJECT
- REVISION CLOUD

ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD
3	02.07.18	RE-ISSUED FOR APPROVAL	SAA	PLP	NH	AA
2	17.05.18	RE-ISSUED FOR APPROVAL	SJM	JLK	NH	AA
1	16.01.18	ISSUED FOR APPROVAL	SAA	JLK	NH	AA
0	17.12.17	ISSUED FOR REVIEW	SAA	JLK	NH	AA

CLIENT	 Dubai Electricity & Water Authority	DEWA PRJ REF : RFX-2131600072 DEWA PO REF : PO: 3761700080 DEWA DWG. NO. RFX72-SRV-LAY3
PROJECT:	SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX - PHASE-3 LAYOUT DRAWING	

VENDOR	 P.O. BOX: 17910, JEBEL ALI, DUBAI, U.A.E. T: +971 (4) 8995000, F: +971 (4) 8995001 www.silvertech-me.com	SCALE: 1: 60 SIZE: A3
STME DWG. NO. PRJ212-PH3-INS-LAY-0001	SHEET 03 OF 03	REV. 3

SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX

PHASE-4 LAYOUT DRAWING (EMERGENCY CENTER)

PRJ212-PH4-INS-LAY-0001-01

REFERENCE DRAWINGS/DOCUMENTS:							<div>CLIENT</div> <div><div><div>هيئة كهرباء ومياه دبي</div><div>Dubai Electricity & Water Authority</div></div><div></div><div><div>P.O. BOX: 564, DUBAI, UAE. TEL: 00971-4-324 4444, FAX: 00971-4-324 4922</div></div></div> <div><div>DEWA PRJ REF : RFX-2131600072</div><div>DEWA PO REF : PO: 3761700080</div></div> <div><div>DEWA DWG. NO.</div><div>RFX72-SRV-LAY4</div></div>	<div>VENDOR</div> <div><div></div><div><div>Silvertech</div><div>PROVIDING THE BEST SOLUTIONS FOR YOUR BUSINESS</div></div><div><div>P.O. BOX: 17910, JEBEL ALI, DUBAI, U.A.E</div><div>T: +971 (4) 8995000, F: +971 (4) 8995001</div><div>www.silvertech-me.com</div></div></div> <div>SCALE: N.T.S.</div> <div>SIZE: A3</div>						
	1	16.01.18	ISSUED FOR CONSTRUCTION	SAA	JLK	NH				AA	PROJECT: SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX - PHASE-4 LAYOUT DRAWING	STME DWG. NO. PRJ212-PH4-INS-LAY-0001	SHEET 01 OF 03	REV. 1
	0	17.12.17	ISSUED FOR REVIEW	SAA	JLK	NH				AA				
	ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD				APRVD				

PRJ212-PH4-INS-LAY-0001-02

SHEET NO.	DESCRIPTION	FILE NAME	DATE	REVISIONS				PURPOSE OF ISSUE
				0	1	2	3	
1	PHASE-4 LAYOUT DRAWING - COVER SHEET	PRJ212-PH4-INS-LAY-0001-01	16.01.18	X	X			ISSUED FOR CONSTRUCTION
2	PHASE-4 LAYOUT DRAWING - INDEX SHEET	PRJ212-PH4-INS-LAY-0001-02	16.01.18	X	X			ISSUED FOR CONSTRUCTION
3	PHASE-4 LAYOUT DRAWING	PRJ212-PH4-INS-LAY-0001-03	16.01.18	X	X			ISSUED FOR CONSTRUCTION
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								
17								
18								
19								
20								
21								
22								
23								
24								
25								
26								
27								
28								
29								
30								
31								
32								
33								
34								
35								
36								
37								
38								

REFERENCE DRAWINGS/DOCUMENTS:

1	16.01.18	ISSUED FOR CONSTRUCTION	SAA	JLK	NH	AA	
0	17.12.17	ISSUED FOR REVIEW	SAA	JLK	NH	AA	
ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD	

CLIENT

هيئة كهرباء ومياه دبي

Dubai Electricity & Water Authority



P.O. BOX: 564, DUBAI, UAE. TEL: 00971-4-324 4444. FAX: 00971-4-324 4922

DEWA PRJ REF : RFX-2131600072


DEWA PO REF : PO: 3761700080

DEWA DWG. NO.

RFX72-SRV-LAY4

PROJECT:
SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA
SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY
IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX - PHASE-4 LAYOUT DRAWING

VENDOR



Silvertech

شركة سيلفرتيخ

P.O. BOX: 17910, JEBEL ALI, DUBAI, U.A.E.
T: +971 (4) 8995000, F: +971 (4) 8995001
www.silvertech-me.com

SCALE:

N.T.S.

SIZE:

A3

STME DWG. NO.

PRJ212-PH4-INS-LAY-0001

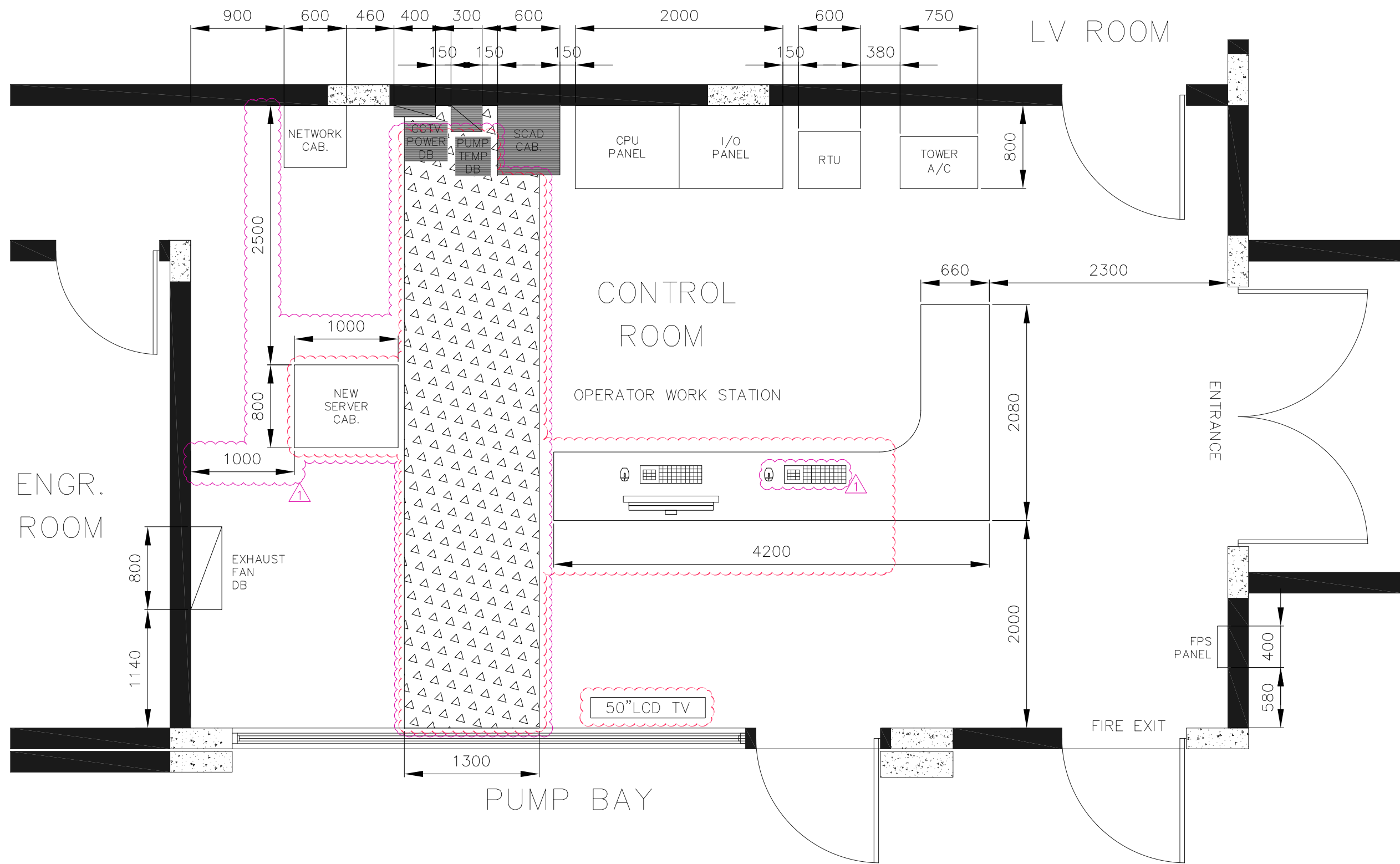
SHEET

02 OF 03

REV.

1

EMERGENCY CENTER



EXISTING NAJMA PUMPING STATION 4 CONTROL ROOM

PRJ212-PH4-INS-LAY-0001-03

REFERENCE DRAWINGS/DOCUMENTS:

LEGEND:-

- SCOPE OF WORK UNDER THIS PROJECT
- REVISION CLOUD

1	16.01.18	ISSUED FOR CONSTRUCTION	SAA	JLK	NH	AA	
0	17.12.17	ISSUED FOR REVIEW	SAA	JLK	NH	AA	
ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD	

CLIENT



DEWA PRJ REF : RFX-2131600072
DEWA PO REF : PO: 3761700080
DEWA DWG. NO.
RFX72-SRV-LAY4

PROJECT:
SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA
SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY
IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX - PHASE-4 LAYOUT DRAWING

VENDOR



P.O. BOX: 17910, JEBEL ALI, DUBAI, U.A.E.
T: +971 (4) 8995000, F: +971 (4) 8995001
www.silverttech-me.com

STME DWG. NO.
PRJ212-PH4-INS-LAY-0001

SHEET
03 OF 03

SCALE:
1 : 40
SIZE:
A3
REV.
1

SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX

GENERAL ARRANGEMENT DRAWING
PHASE-3 SERVER PANEL

REFERENCE DRAWINGS/DOCUMENTS:								<div>CLIENT</div> <div><div><div>هيئة كهرباء ومياه دبي</div><div>Dubai Electricity & Water Authority</div></div><div><div><div></div></div></div><div>P.O. BOX: 564, DUBAI, UAE. TEL: 00971-4-324 4444. FAX: 00971-4-324 4922</div></div> <div><div>DEWA PRJ REF : RFX-2131600072</div><div>DEWA PO REF : PO: 3761700080</div><div>DEWA DWG. NO.</div><div>RFX72-SRV-GAD3</div></div>	<div>VENDOR</div> <div><div><div><div></div></div><div>Silvertech</div><div>Authorised maintenance and repair services provider</div></div><div><div>P.O. BOX: 17910, JEBEL ALI, DUBAI, U.A.E</div><div>T: +971 (4) 8995000, F: +971 (4) 8995001</div><div>www.silvertech-me.com</div></div></div> <div><div>STME DWG. NO.</div><div>PRJ212-PH3-INS-GAD-0001</div></div> <div><div>SHEET</div><div>01 OF 09</div></div> <div><div>SCALE:</div><div>N.T.S.</div><div>SIZE:</div><div>A3</div><div>REV.</div><div>3</div></div>
	3	20.07.18	APPROVED FOR CONSTRUCTION	SJM	PLP	NH	AA		
	2	19.04.18	RE-ISSUED FOR APPROVAL	SJM	JLK	NH	AA		
	1	11.04.18	ISSUED FOR APPROVAL	SJM	JLK	NH	AA		
	0	14.02.18	ISSUED FOR REVIEW	SAA	JLK	NH	AA		
	ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD		

PRJ212-PH3-INS-GAD-0001-02

SHEET NO.	DESCRIPTION	FILE NAME	DATE	REVISIONS				PURPOSE OF ISSUE
				0	1	2	3	
1	PHASE-3 SERVER PANEL GENERAL ARRANGEMENT DRAWING - COVER SHEET	PRJ212-PH3-INS-GAD-0001-01	20.07.18	X	X	X	X	APPROVED FOR CONSTRUCTION
2	PHASE-3 SERVER PANEL GENERAL ARRANGEMENT DRAWING - INDEX SHEET	PRJ212-PH3-INS-GAD-0001-02	20.07.18	X	X	X	X	APPROVED FOR CONSTRUCTION
3	PHASE-3 SERVER PANEL GENERAL ARRANGEMENT DRAWING - LEGEND SHEET	PRJ212-PH3-INS-GAD-0001-03	20.07.18	X	X	X	X	APPROVED FOR CONSTRUCTION
4	PHASE-3 SERVER PANEL GENERAL ARRANGEMENT DRAWING	PRJ212-PH3-INS-GAD-0001-04	20.07.18	X	X	X	X	APPROVED FOR CONSTRUCTION
5	PHASE-3 SERVER PANEL GENERAL ARRANGEMENT DRAWING	PRJ212-PH3-INS-GAD-0001-05	20.07.18	X	X	X	X	APPROVED FOR CONSTRUCTION
6	PHASE-3 SERVER PANEL GENERAL ARRANGEMENT DRAWING	PRJ212-PH3-INS-GAD-0001-06	20.07.18	X	X	X	X	APPROVED FOR CONSTRUCTION
7	PHASE-3 SERVER PANEL GENERAL ARRANGEMENT DRAWING - LABEL DETAILS	PRJ212-PH3-INS-GAD-0001-07	20.07.18	X	X	X	X	APPROVED FOR CONSTRUCTION
8	PHASE-3 SERVER PANEL GENERAL ARRANGEMENT DRAWING - BILL OF MATERIALS	PRJ212-PH3-INS-GAD-0001-08	20.07.18	X	X	X	X	APPROVED FOR CONSTRUCTION
9	PHASE-3 SERVER PANEL GENERAL ARRANGEMENT DRAWING - BILL OF MATERIALS	PRJ212-PH3-INS-GAD-0001-09	20.07.18	X	X	X	X	APPROVED FOR CONSTRUCTION
10								
11								
12								
13								
14								
15								
16								
17								
18								
19								
20								
21								
22								
23								
24								
25								
26								
27								
28								
29								
30								
31								
32								
33								
34								
35								
36								
37								
38								

REFERENCE DRAWINGS/DOCUMENTS:

3	20.07.18	APPROVED FOR CONSTRUCTION	SJM	PLP	NH	AA	
2	19.04.18	RE-ISSUED FOR APPROVAL	SJM	JLK	NH	AA	
1	11.04.18	ISSUED FOR APPROVAL	SJM	JLK	NH	AA	
0	14.02.18	ISSUED FOR REVIEW	SAA	JLK	NH	AA	
ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD	


CLIENT	<div><div>هيئة كهرباء ومياه دبي</div><div>Dubai Electricity & Water Authority</div><div></div></div>	DEWA PRJ REF : RFX-2131600072
		DEWA PO REF : PO: 3761700080
		DEWA DWG. NO. RFX72-SRV-GAD3
P.O. BOX: 564, DUBAI, UAE TEL: 00971-4-324 4444. FAX: 00971-4-324 4922		
PROJECT:		
SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA		
SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY		
IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX - PHASE-3 SERVER PANEL GA DRAWING-INDEX SHEET		



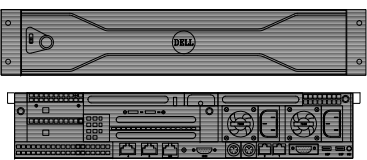
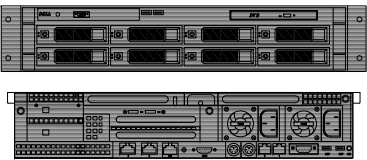




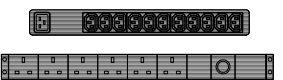
VENDOR	<div><div></div><div>Silvertech</div><div>Authorised Engineering & Technology Company</div><div>P.O. BOX: 17910, JEBEL ALI, DUBAI, U.A.E</div><div>T. +971 (4) 8995000, F. +971 (4) 8995001</div><div>www.silvertech-me.com</div></div>	

STME DWG. NO.	SHEET
PRJ212-PH3-INS-GAD-0001	02 OF 09

SCALE:
N.T.S.
SIZE:
A3
REV:
3

SYMBOLS LEGEND:

	MINIATURE CIRCUIT BREAKER
	DOOR SWITCH
	TERMINAL BLOCKS
	ETHERNET TCP/IP MANAGED SWITCH
	POWER SUPPLY UNIT
	REDUNDANCY MODULE
	KVM EXTENDER (CE750)
	CMC III BUS ACCESS
	CMC III PROCESSING UNIT
	PE & IE BAR
	CMC III READER UNITS
	FAN
	FILTER

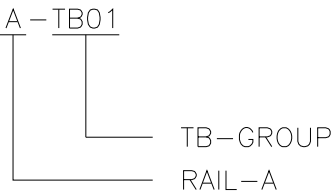
	CMC III MOUNTING UNITS
	ETHERNET MANAGED SWITCH (EXTREME X440-G2-24t-10GE4)
	WORK STATION
	SERVER
	KVM SWITCH WITH MONITOR
	CABLE MANAGEMENT
	1U BLANK PLATE
	COMPACT LIGHT
	POWER DISTRIBUTION UNIT (PDU)

LEGENDS:

CB	: MINIATURE CIRCUIT BREAKER
DS	: DOOR SWITCH
ES	: ETHERNET SWITCH (EXTREME B5)
LT	: PANEL LIGHT
PDU	: POWER DISTRIBUTION UNIT
SE	: SAFETY EARTH
IE	: INSTRUMENT EARTH
ESW	: ETHERNET SWITCH
TB	: TERMINAL BLOCKS
OVS	: OPERATOR WORKSTATION SERVER
EWS	: ENGINEERING WORKSTATION SERVER
PU	: PROCESSING UNITS
RU	: READER UNIT
BA	: BUS ACCESS
CT	: CABLE TRAY

NAMING CONVENTION:

RAIL:



REFERENCE DRAWINGS/DOCUMENTS:

3	20.07.18	APPROVED FOR CONSTRUCTION	SJM	PLP	NH	AA	
2	19.04.18	RE-ISSUED FOR APPROVAL	SJM	JLK	NH	AA	
1	11.04.18	ISSUED FOR APPROVAL	SJM	JLK	NH	AA	
0	14.02.18	ISSUED FOR REVIEW	SAA	JLK	NH	AA	
ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD	

CLIENT		DEWA PRJ REF : RFX-2131600072 DEWA PO REF : PO: 3761700080 DEWA DWG. NO. RFX72-SRV-GAD3
PROJECT:	SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX - PHASE-3 SERVER PANEL GA DRAWING - LEGEND SHEET	

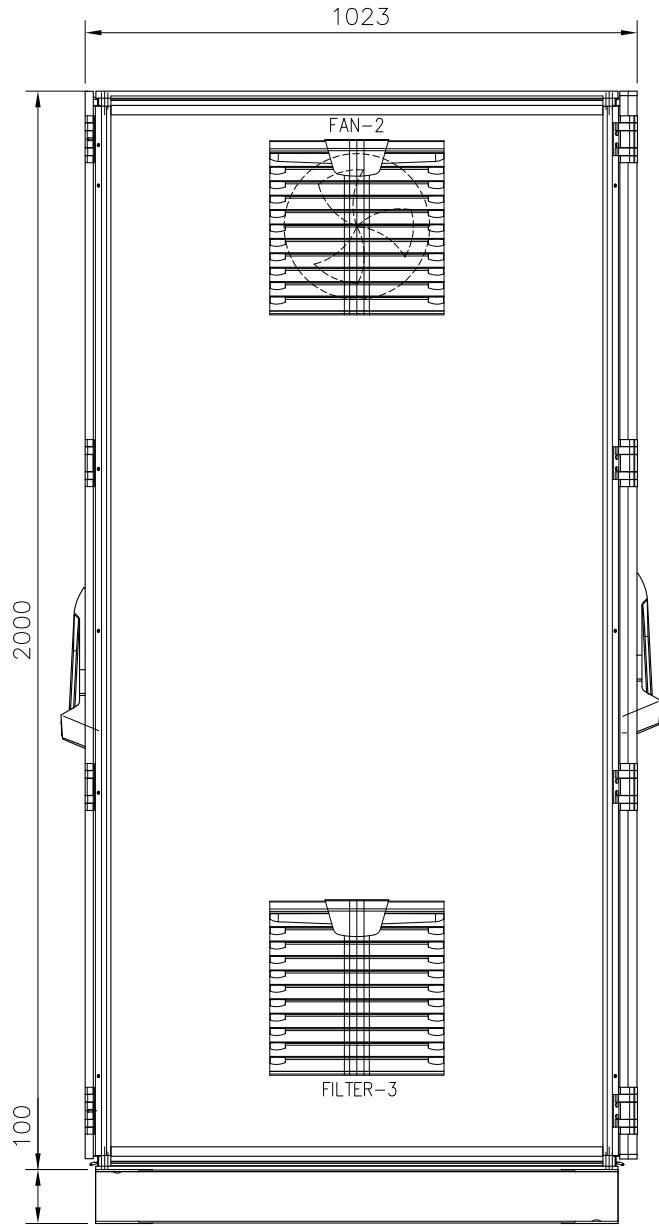
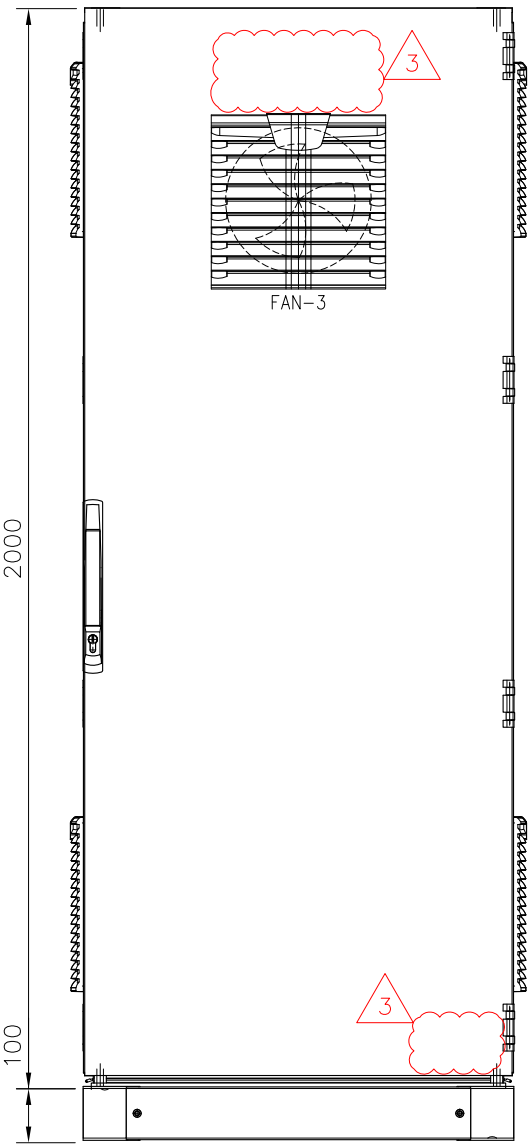
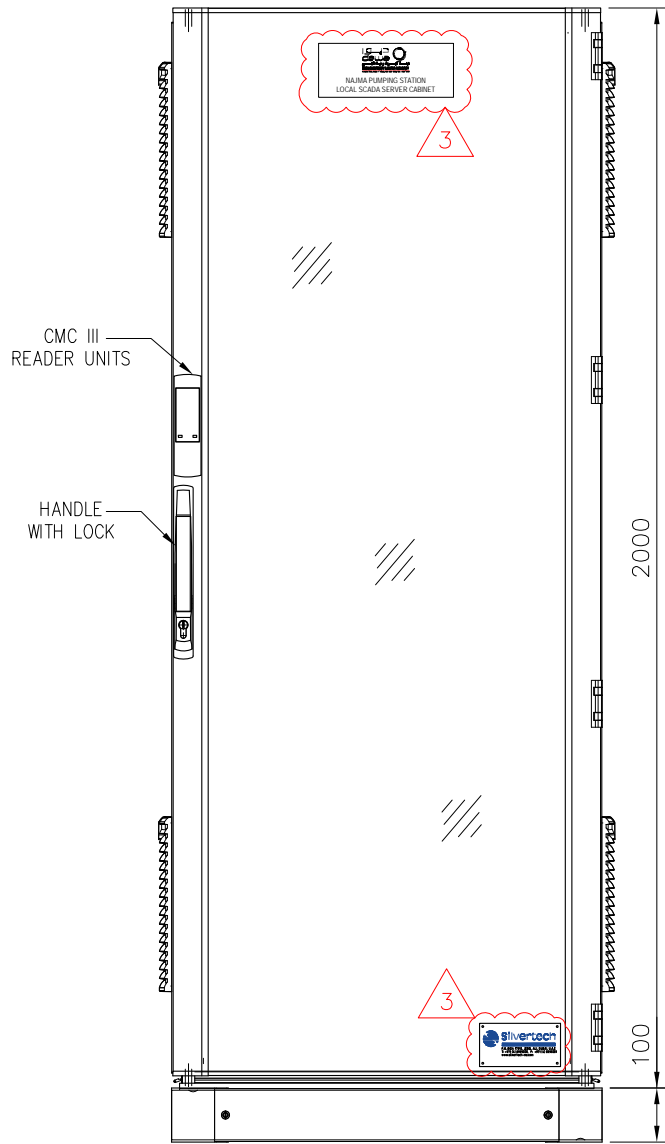
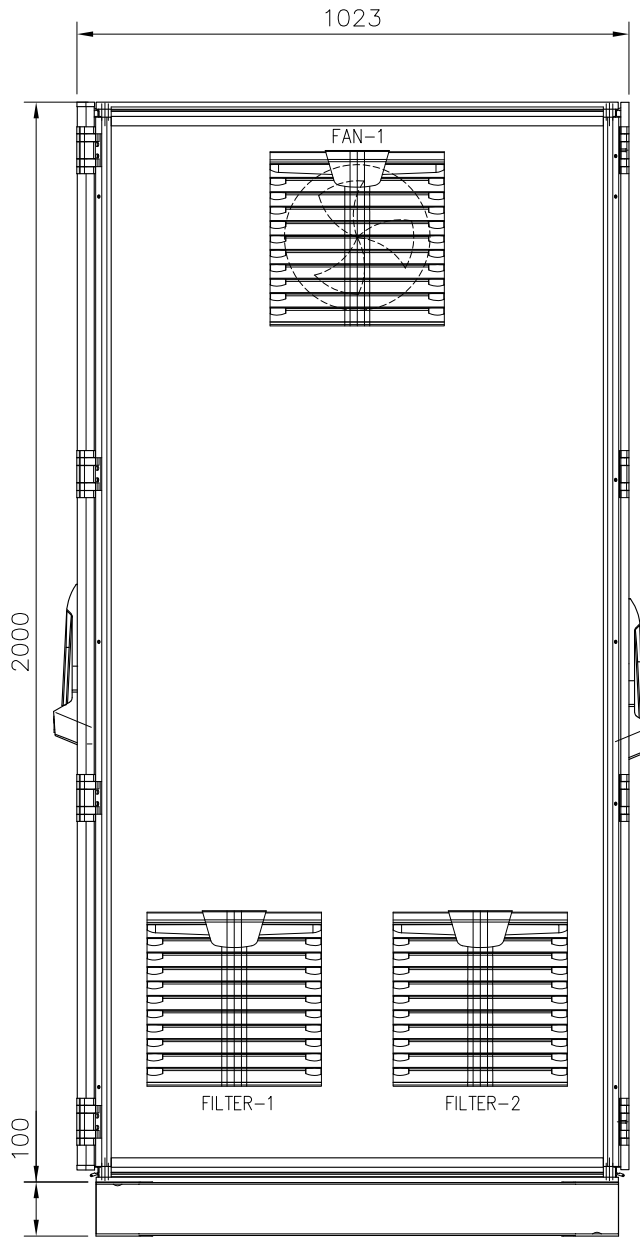
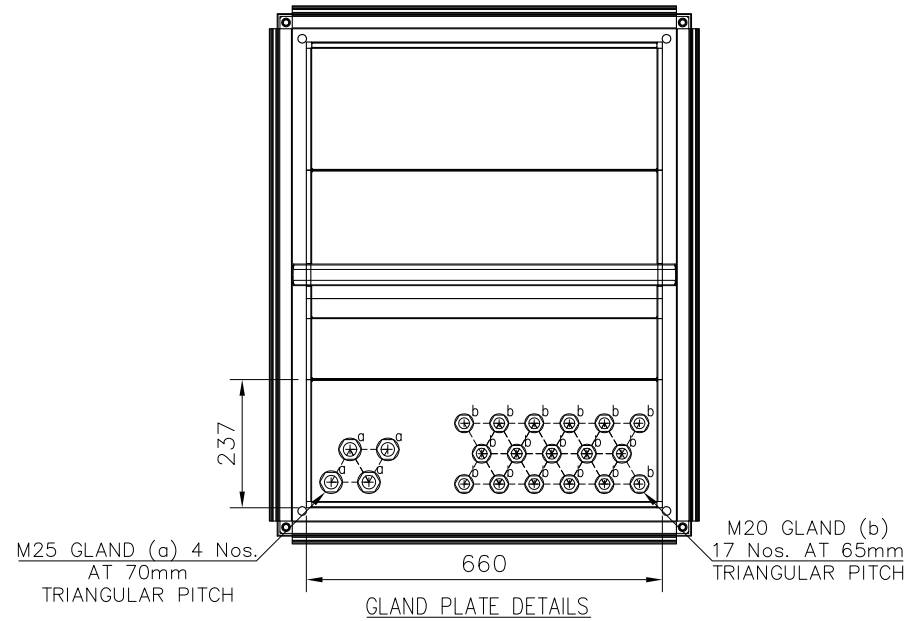
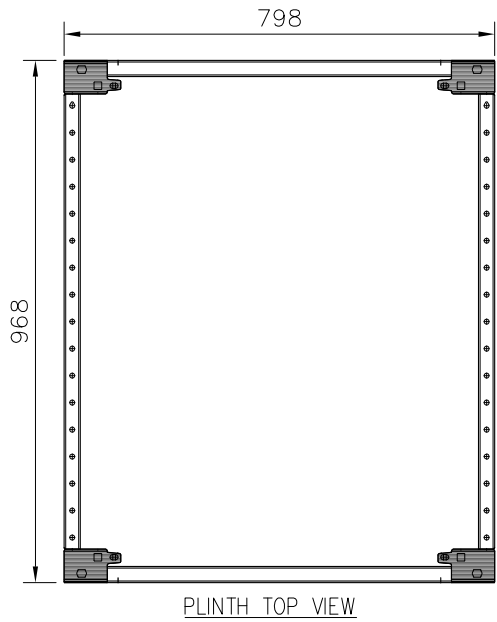
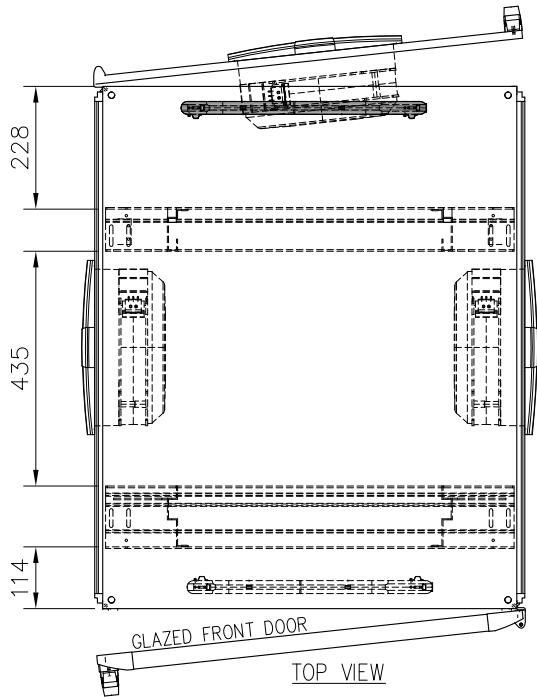
VENDOR	
P.O. BOX: 17910, JEBEL ALI, DUBAI, U.A.E T: +971 (4) 8995000, F: +971 (4) 8995001 www.silvertech-me.com	

STME DWG. NO.	SHEET
PRJ212-PH3-INS-GAD-0001	03 OF 09

SCALE:	N.T.S.
SIZE:	A3
REV.	3

NOTES:

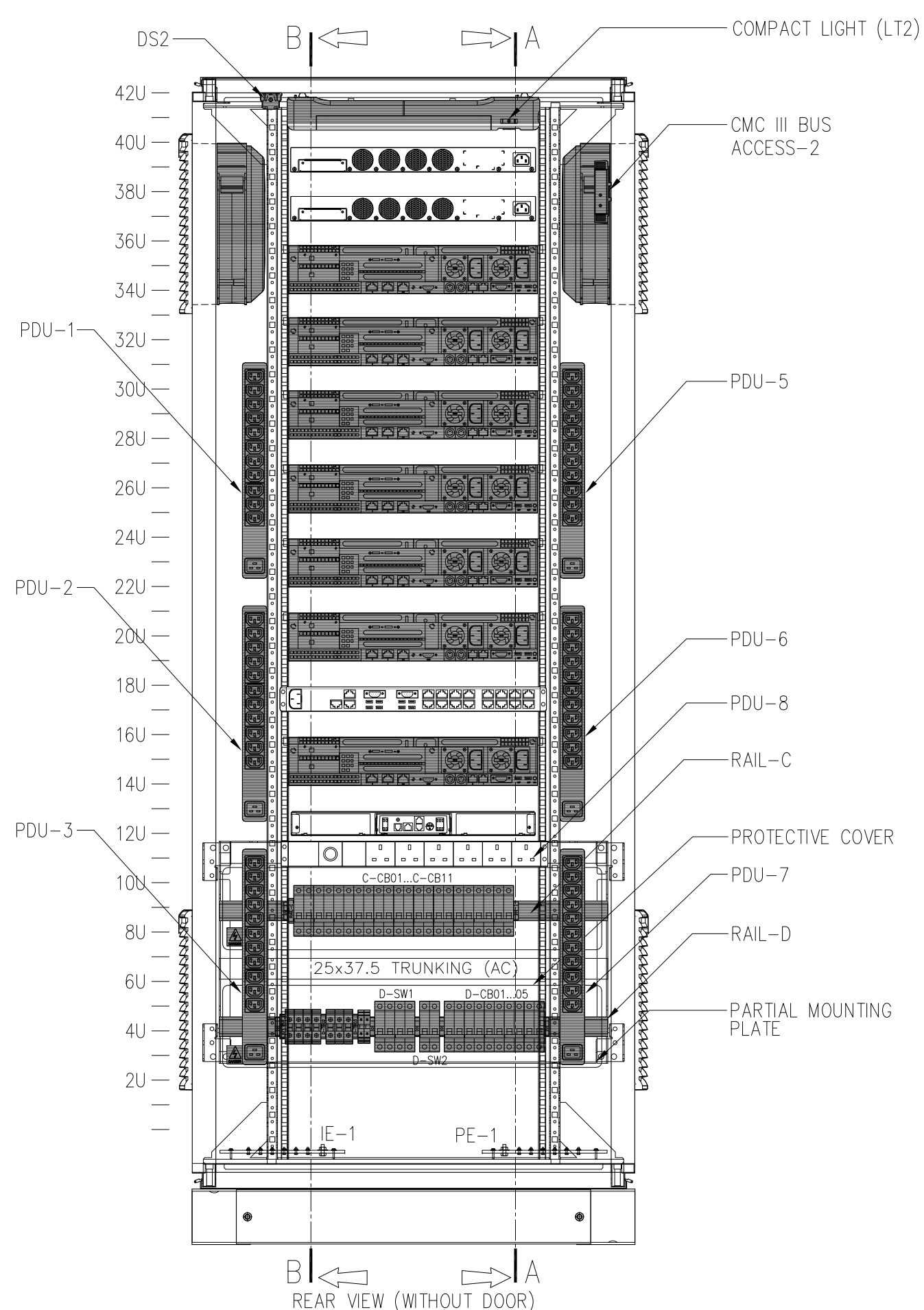
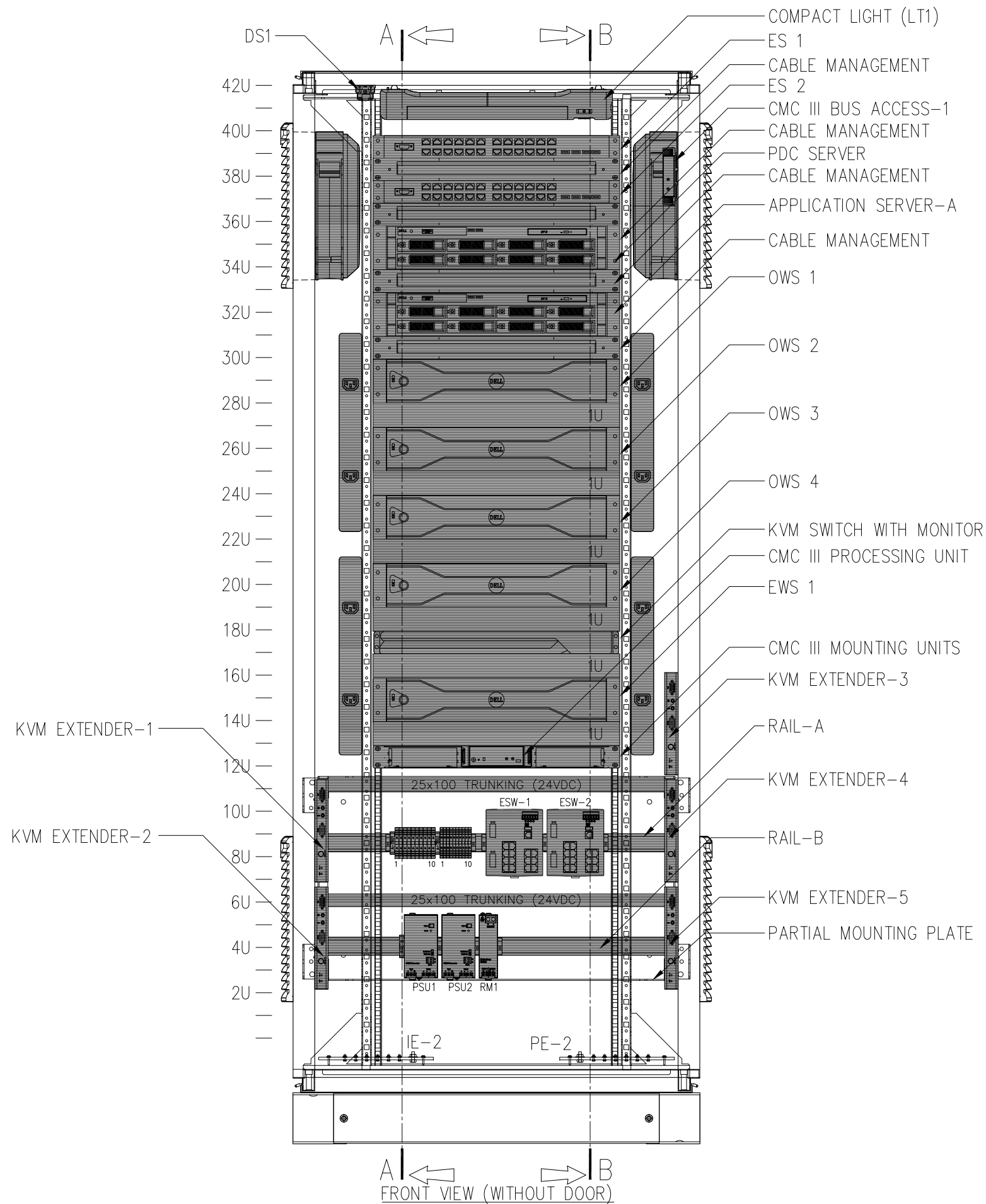
1. RITTAL ENCLOSURE: TS SERIES (WITH FRONT AND REAR DOOR) DOOR:
FRONT: GLAZED ALUMINIUM DOOR, 180° HINGES
REAR: SHEET STEEL DOOR, 180° HINGES
2. FINISH : RAL 7035
MOUNTING PLATE: ZINC-PLATED
INTERIOR INSTALLATION: RAL 9005
3. CABLE ENTRY IS THROUGH THE BOTTOM OF THE ENCLOSURE.
4. PANEL IS FRONT AND REAR ACCESS
5. ESTIMATED WEIGHT : - 450KG.
6. ALL DIMENSIONS ARE IN "mm"



REFERENCE DRAWINGS/DOCUMENTS:

3	20.07.18	APPROVED FOR CONSTRUCTION	SJM	PLP	NH	AA
2	19.04.18	RE-ISSUED FOR APPROVAL	SJM	JLK	NH	AA
1	11.04.18	ISSUED FOR APPROVAL	SJM	JLK	NH	AA
0	14.02.18	ISSUED FOR REVIEW	SAA	JLK	NH	AA
ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD

CLIENT	DEWA PRJ REF : RFX-2131600072 DEWA PO REF : PO: 3761700080 DEWA DWG. NO. RFX72-SRV-GAD3	VENDOR	SCALE: 1 : 15 SIZE: A3 REV: 3
PROJECT:	SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX - PHASE-3 SERVER PANEL GA DRAWING	STME DWG. NO.	SHEET
		PRJ212-PH3-INS-GAD-0001	04 OF 09



REFERENCE DRAWINGS/DOCUMENTS:

3	20.07.18	APPROVED FOR CONSTRUCTION	SJM	PLP	NH	AA
2	19.04.18	RE-ISSUED FOR APPROVAL	SJM	JLK	NH	AA
1	11.04.18	ISSUED FOR APPROVAL	SJM	JLK	NH	AA
0	14.02.18	ISSUED FOR REVIEW	SAA	JLK	NH	AA
ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD

CLIENT

هيئة كهرباء ومياه دبي
Dubai Electricity & Water Authority

P.O. BOX: 564, DUBAI, UAE. TEL: 00971-4-324 4444. FAX: 00971-4-324 4922

DEWA PRJ REF : RFX-2131600072
DEWA PO REF : PO: 3761700080
DEWA DWG. NO.
RFX72-SRV-GAD3

PROJECT:

SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA
SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY
IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX - PHASE-3 SERVER PANEL GA DRAWING

VENDOR

Silvertech
P.O. BOX: 17910, JEBEL ALI, DUBAI, U.A.E
T: +971 (4) 8995000, F: +971 (4) 8995001
www.silvertech-me.com

STME DWG. NO.

PRJ212-PH3-INS-GAD-0001

SHEET

05 OF 09

SCALE:

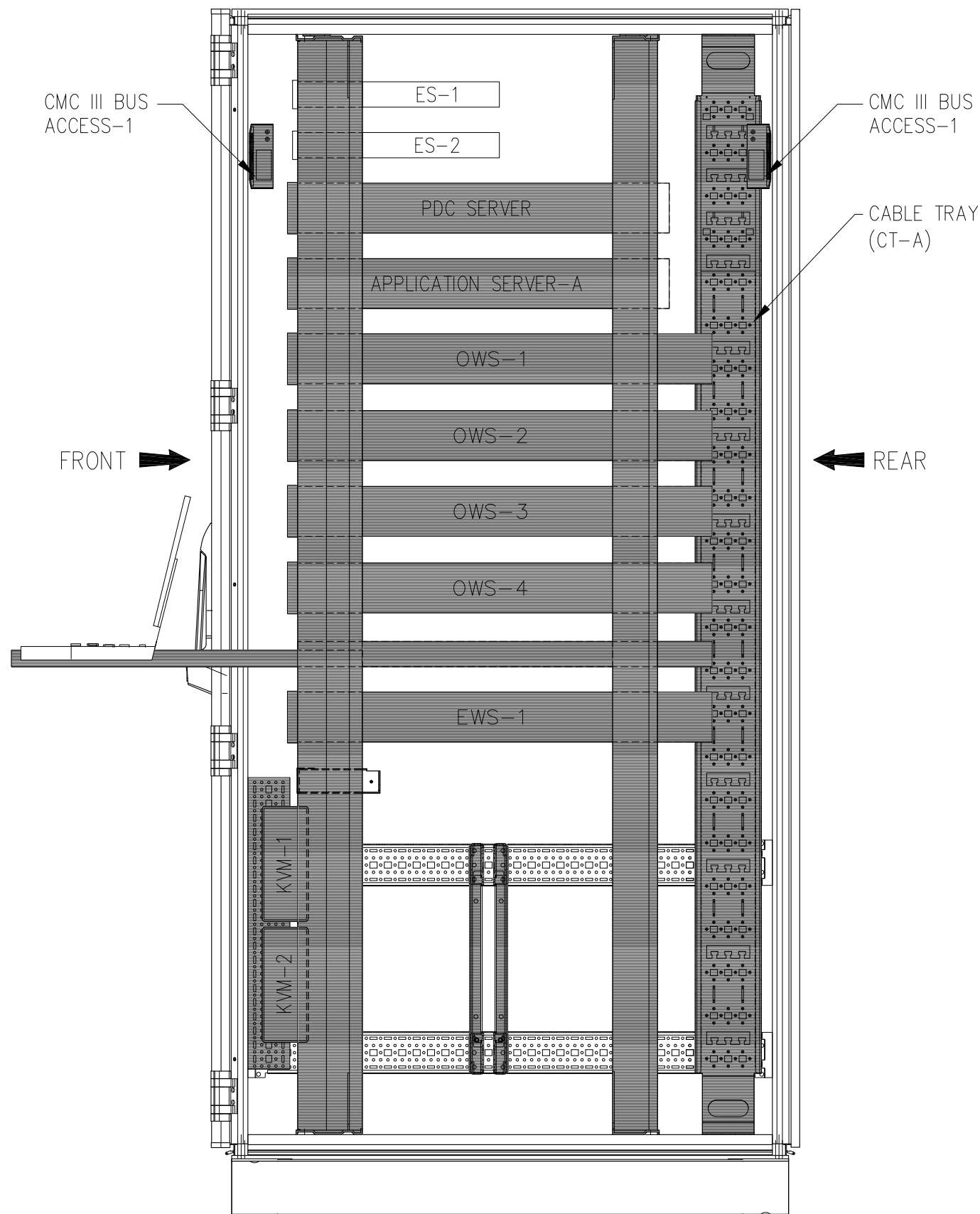
1 : 10

SIZE:

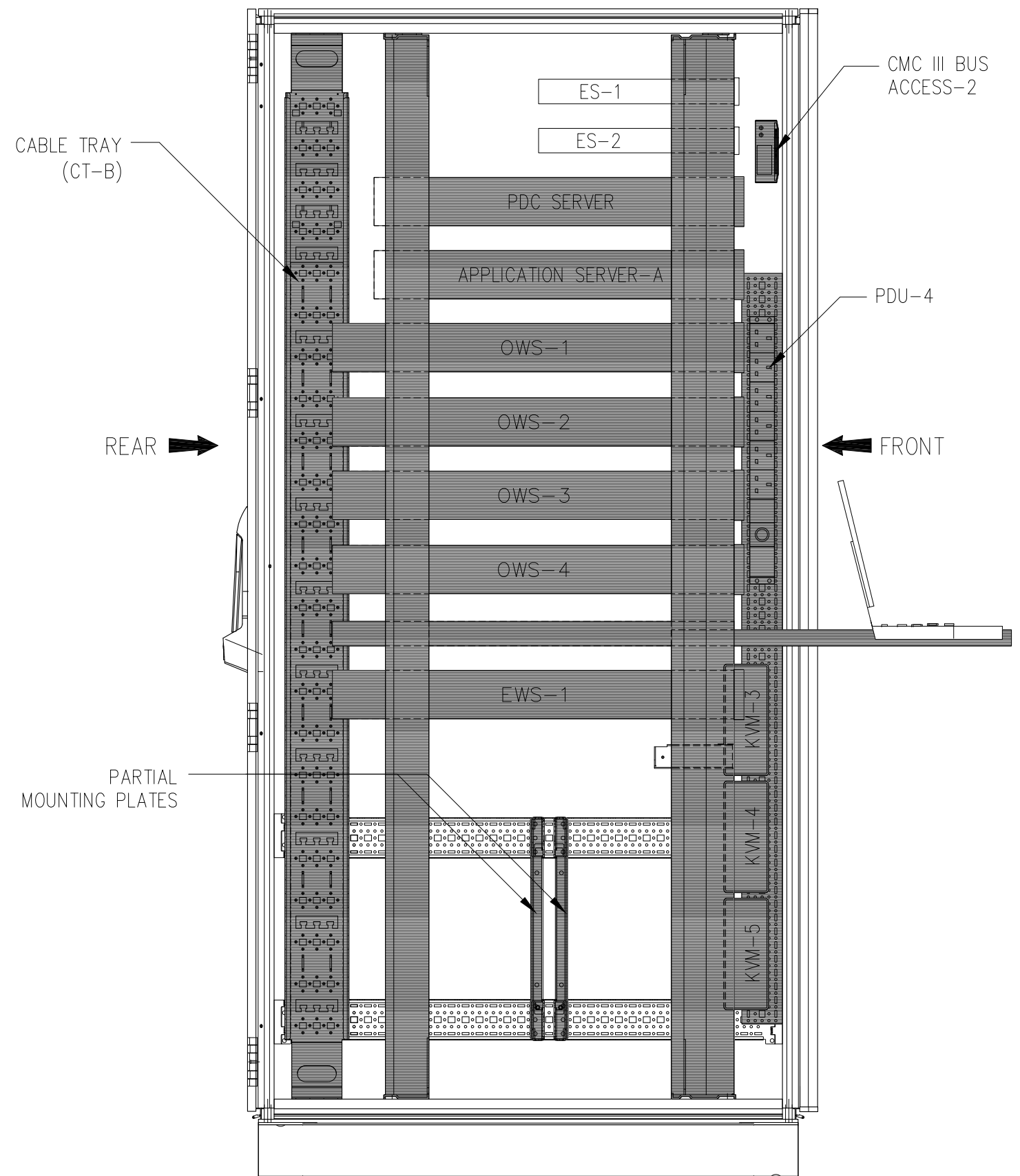
A3

REV.

3





"A-A" VIEW



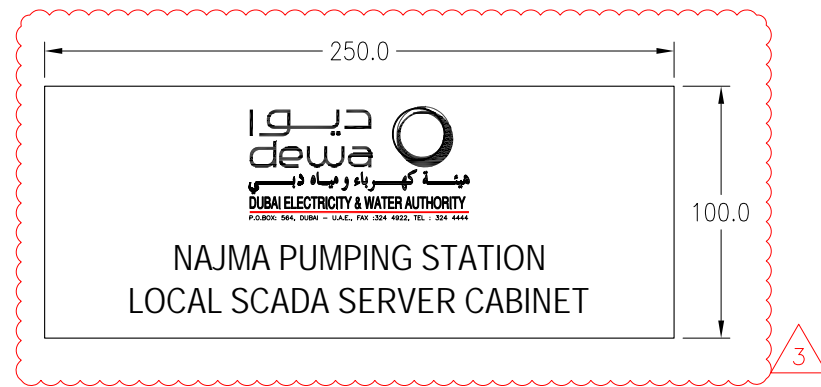
"B-B" VIEW

REFERENCE DRAWINGS/DOCUMENTS:

3	20.07.18	APPROVED FOR CONSTRUCTION	SJM	PLP	NH	AA
2	19.04.18	RE-ISSUED FOR APPROVAL	SJM	JLK	NH	AA
1	11.04.18	ISSUED FOR APPROVAL	SJM	JLK	NH	AA
0	14.02.18	ISSUED FOR REVIEW	SAA	JLK	NH	AA
ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD

CLIENT	 هيئة كهرباء ومياه دبي Dubai Electricity & Water Authority	DEWA PRJ REF : RFX-2131600072 DEWA PO REF : PO: 3761700080 DEWA DWG. NO. RFX72-SRV-GAD3	VENDOR	 Silvertech P.O. BOX: 17910, JEBEL ALI, DUBAI, U.A.E T : +971 (4) 8995000, F : +971 (4) 8995001 www.silvertech-me.com	SCALE:
					1 : 10
P.O. BOX: 564, DUBAI, UAE. TEL: 00971-4-324 4444. FAX: 00971-4-324 4922	PROJECT: SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX - PHASE-3 SERVER PANEL GA DRAWING			SIZE:	
				A3	
	STME DWG. NO. PRJ212-PH3-INS-GAD-0001		SHEET 06 OF 09	REV. 3	

ENCLOSURE LABEL



MATERIAL : STAINLESS STEEL 316L 1.6mm
LABEL : COLOR LASER PRINTED AND LAMINATED
TEXT HEIGHT : 10mm.

LABEL LOCATION : OUTSIDE
FIXING TYPE : ADHESIVE
TEXT FONT : ARIAL

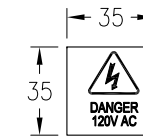
MANUFACTURER LABEL



MATERIAL : STAINLESS STEEL 316L 1.6mm
LABEL : ENGRAVED, INK FILLED AND LAMINATED
TEXT COLOR : BLACK

LABEL LOCATION : OUTSIDE
FIXING TYPE : ADHESIVE

WARNING LABEL

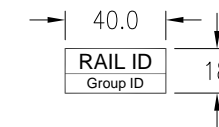


LABEL BACKGROUND : YELLOW
TEXT COLOR : BLACK
TEXT HEIGHT : 4mm.

LABEL LOCATION : INSIDE
FIXING TYPE : ADHESIVE

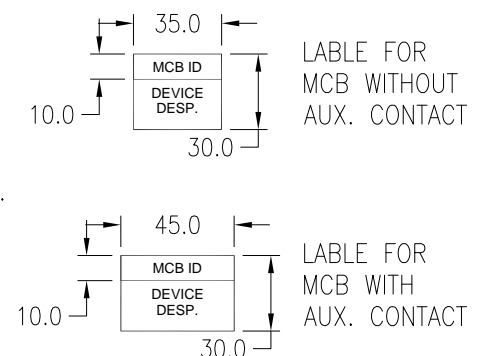
TYPICAL TERMINAL GROUP MARKER

LABEL BACKGROUND : WHITE
TEXT COLOR : BLACK
TEXT HEIGHT 1ST LINE : 6mm.
TEXT HEIGHT 2ND LINE : 4mm.
LABEL LOCATION : INSIDE
FIXING TYPE : ADHESIVE



TYPICAL MCB LABEL

LABEL BACKGROUND : WHITE
TEXT COLOR : BLACK
TEXT HEIGHT 1ST LINE : 4mm.
TEXT HEIGHT 2ND LINE : 4mm.
LABEL LOCATION : INSIDE
FIXING TYPE : ADHESIVE



REFERENCE DRAWINGS/DOCUMENTS:

ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD
3	20.07.18	APPROVED FOR CONSTRUCTION	SJM	PLP	NH	AA
2	19.04.18	RE-ISSUED FOR APPROVAL	SJM	JLK	NH	AA
1	11.04.18	ISSUED FOR APPROVAL	SJM	JLK	NH	AA
0	14.02.18	ISSUED FOR REVIEW	SAA	JLK	NH	AA

CLIENT	DEWA PRJ REF : RFX-2131600072 DEWA PO REF : PO: 3761700080 DEWA DWG. NO. RFX72-SRV-GAD3
PROJECT:	SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX - PHASE-3 SERVER PANEL GA DRAWING-LABEL DETAILS

VENDOR	SCALE: N.T.S.
STME DWG. NO. PRJ212-PH3-INS-GAD-0001	SHEET 07 OF 09
REV. 3	SIZE: A3

SR NO.	TAGS	DESCRIPTION	MANUFACTURER	PART No.	QTY.
1	-	ENCLOSURE (800W X 1000D X 2000H) WITH FRONT GLAZED DOOR & REAR STEEL DOOR	RITTAL	DK 5509.131	01 No.
2	FAN1....FAN3	FAN	RITTAL	3245.500	03 Nos.
3					
4	-	FILTER	RITTAL	SK 3243.200	04 Nos.
5	LT1, LT2	COMPACT LIGHT	RITTAL	SZ 4140.010	02 Nos.
6	DS1, DS2	DOOR SWITCH	RITTAL	SZ 4127.010	02 Nos.
7	-	FRONT & REAR PANEL (PLINTH)	RITTAL	TS 8601.805	1 SET
8	-	PANEL PLINTH	RITTAL	TS 8601.015	1 SET
9	-	HANDLE WITH SEMI CYLINDER	RITTAL	DK 7320.721 + SZ 2467.000	02 Nos.
10	RU-1	CMC III READER UNITS	RITTAL	DK 7030.230	01 No.
11	-	PDC SERVER (2U FORM FACTOR)	DELL	POWER EDGE R530	01 No.
12	-	APPLICATION SERVER-A (2U FORM FACTOR)	DELL	POWER EDGE R530	01 No.
13	ES 1 - ES 2	MANAGED ETHERNET SWITCH	EXTREME	X440-G2-24t-10GE4	02 Nos.
14	OWS 1 - OWS 4	OPERATOR WORKSTATION SERVER (2U FORM FACTOR)	DELL	PRECISION 7910	04 Nos.
15	-	DAV2216-G01 KVM SWITCH + 1U RACKMOUNT LED CONSOLE	DELL	A7485896 + FPM185	01 No.
16	EWS 1	ENGINEERING WORKSTATION SERVER (2U FORM FACTOR)	DELL	PRECISION 7920	01 No.
17	PU-1	CMC III PROCESSING UNITS	RITTAL	DK 7030.010	01 No.
18	-	CMC III MOUNTING UNIT	RITTAL	DK 7030.070	01 No.
19	-	1U 19" BLANK PLATE	RITTAL	DK 7151.005	06 Nos.
20	-	19" CABLE MANAGEMENT PANEL WITH BRUSH STRIP	RITTAL	DK-5502.265	04 Nos.
21	KVM1 - KVM5	KVM EXTENDER	ATEN	CE750	05 Nos.
22	BA-1 & BA-2	CMC III CAN BUS ACCESS	RITTAL	DK 7030.200	02 Nos.
		RAIL-A			
23	A-TB1	FUSE TERMINAL (WSI 6)	WEIDMULLER	1011000000	10 Nos.
24	A-TB2	FEED THROUGH TERMINAL (WDU 4)	WEIDMULLER	1020100000	10 Nos.
25	ESW1 - ESW2	ETHERNET TCP/IP MANAGED SWITCH - CONNEXIUM-14TX/2FX - SINGLE MODE	SCHNEIDER ELECTRIC	TCSESM163F2CS0	02 Nos.
		RAIL-B			
26	PSU1 & PSU2	POWER SUPPLY 200V-240V AC/24V 28V DC 20A	PULS	CPS20.241-C1	02 Nos.
27	RM1	DUAL REDUNDANCY MODULE 12-28V, 40A	PULS	YR40.242	01 No.
		RAIL-C			
28	C-CB1	MCB 16A 2P	SCHNEIDER ELECTRIC	A9F44216	01 No.
29	C-CB2 - C-CB4	MCB 10A 2P	SCHNEIDER ELECTRIC	A9F44210	03 Nos.
30	C-CB5 - C-CB8	MCB 4A 2P	SCHNEIDER ELECTRIC	A9F44204	04 Nos.
31	C-CB9 - C-CB11	MCB 2A 2P	SCHNEIDER ELECTRIC	A9F44202	03 Nos.

REFERENCE DRAWINGS/DOCUMENTS:

3	20.07.18	APPROVED FOR CONSTRUCTION	SJM	PLP	NH	AA	
2	19.04.18	RE-ISSUED FOR APPROVAL	SJM	JLK	NH	AA	
1	11.04.18	ISSUED FOR APPROVAL	SJM	JLK	NH	AA	
0	14.02.18	ISSUED FOR REVIEW	SAA	JLK	NH	AA	
ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD	

CLIENT

هيئة كهرباء ومياه دبي
Dubai Electricity & Water Authority




P.O. BOX: 564, DUBAI, UAE TEL: 00971-4-324 4444 FAX: 00971-4-324 4922

DEWA PRJ REF : RFX-2131600072
DEWA PO REF : PO: 3761700080

DEWA DWG. NO.
RFX72-SRV-GAD3

PROJECT:
SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA
SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY
IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX - PHASE-3 SERVER PANEL BOM

VENDOR



Silvertech
P.O. BOX: 17910, JEBEL ALI, DUBAI, U.A.E
T. +971 (4) 8995000, F. +971 (4) 8995001
www.silvertech-me.com

STME DWG. NO.
PRJ212-PH3-INS-GAD-0001

SHEET
08 OF 09

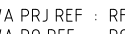

SCALE:
N.T.S.

SIZE:
A3

REV:
3

SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX

GENERAL ARRANGEMENT DRAWING
PHASE-4 SERVER PANEL

REFERENCE DRAWINGS/DOCUMENTS:								CLIENT <div><div>هيئة كهرباء ومياه دبي</div><div>Dubai Electricity & Water Authority</div><div></div><div>P.O. BOX: 564, DUBAI, UAE. TEL: 00971-4-324 4444. FAX: 00971-4-324 4922</div></div>	DEWA PRJ REF : RFX-2131600072 DEWA PO REF : PO: 3761700080 DEWA DWG. NO. RFX72-SRV-GAD4	VENDOR <div><div> Silvertech</div><div><div>P.O. BOX: 17910, JEBEL ALI, DUBAI, U.A.E</div><div>T: +971 (4) 8995000, F: +971 (4) 8995001</div><div>www.silvertech-me.com</div></div></div>	SCALE: N.T.S.
	3	20.07.18	APPROVED FOR CONSTRUCTION	SJM	PLP	NH	AA				
	2	19.04.18	RE-ISSUED FOR APPROVAL	SJM	JLK	NH	AA				
	1	11.04.18	ISSUED FOR APPROVAL	SJM	JLK	NH	AA				
	0	15.02.18	ISSUED FOR REVIEW	SAA	JLK	NH	AA				
		ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD	PROJECT: SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX - PHASE-4 SERVER PANEL GA DRAWING - COVER SHEET	STME DWG. NO. PRJ212-PH4-INS-GAD-0001	SHEET 01 OF 09

PRJ212-PH4-INS-GAD-0001-02

SHEET NO.	DESCRIPTION	FILE NAME	DATE	REVISIONS				PURPOSE OF ISSUE
				0	1	2	3	
1	PHASE-4 SERVER PANEL GENERAL ARRANGEMENT DRAWING - COVER SHEET	PRJ212-PH4-INS-GAD-0001-01	20.07.18	X	X	X	X	APPROVED FOR CONSTRUCTION
2	PHASE-4 SERVER PANEL GENERAL ARRANGEMENT DRAWING - INDEX SHEET	PRJ212-PH4-INS-GAD-0001-02	20.07.18	X	X	X	X	APPROVED FOR CONSTRUCTION
3	PHASE-4 SERVER PANEL GENERAL ARRANGEMENT DRAWING - LEGEND SHEET	PRJ212-PH4-INS-GAD-0001-03	20.07.18	X	X	X	X	APPROVED FOR CONSTRUCTION
4	PHASE-4 SERVER PANEL GENERAL ARRANGEMENT DRAWING	PRJ212-PH4-INS-GAD-0001-04	20.07.18	X	X	X	X	APPROVED FOR CONSTRUCTION
5	PHASE-4 SERVER PANEL GENERAL ARRANGEMENT DRAWING	PRJ212-PH4-INS-GAD-0001-05	20.07.18	X	X	X	X	APPROVED FOR CONSTRUCTION
6	PHASE-4 SERVER PANEL GENERAL ARRANGEMENT DRAWING	PRJ212-PH4-INS-GAD-0001-06	20.07.18	X	X	X	X	APPROVED FOR CONSTRUCTION
7	PHASE-4 SERVER PANEL GENERAL ARRANGEMENT DRAWING - LABEL DETAILS	PRJ212-PH4-INS-GAD-0001-07	20.07.18	X	X	X	X	APPROVED FOR CONSTRUCTION
8	PHASE-4 SERVER PANEL GENERAL ARRANGEMENT DRAWING - BILL OF MATERIALS	PRJ212-PH4-INS-GAD-0001-08	20.07.18	X	X	X	X	APPROVED FOR CONSTRUCTION
9	PHASE-4 SERVER PANEL GENERAL ARRANGEMENT DRAWING - BILL OF MATERIALS	PRJ212-PH4-INS-GAD-0001-09	20.07.18	X	X	X	X	APPROVED FOR CONSTRUCTION
10								
11								
12								
13								
14								
15								
16								
17								
18								
19								
20								
21								
22								
23								
24								
25								
26								
27								
28								
29								
30								
31								
32								
33								
34								
35								
36								
37								
38								

REFERENCE DRAWINGS/DOCUMENTS:

3	20.07.18	APPROVED FOR CONSTRUCTION	SJM	PLP	NH	AA	
2	19.04.18	RE-ISSUED FOR APPROVAL	SJM	JLK	NH	AA	
1	11.04.18	ISSUED FOR APPROVAL	SJM	JLK	NH	AA	
0	15.02.18	ISSUED FOR REVIEW	SAA	JLK	NH	AA	
ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD	

CLIENT

هيئة كهرباء ومياه دبي

Dubai Electricity & Water Authority



DEWA PRJ REF : RFX-2131600072

DEWA PO REF : PO: 3761700080

DEWA DWG. NO.

RFX72-SRV-GAD4

P.O. BOX: 564, DUBAI, UAE TEL: 00971-4-324 4444 FAX: 00971-4-324 4922

PROJECT:

SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX - PHASE-4 SERVER PANEL GA DRAWING-INDEX SHEET

VENDOR



Silvertech

Authoring, Engineering, Drafting, Simulation, EPC, Commissioning

P.O. BOX: 17910, JEBEL ALI, DUBAI, U.A.E




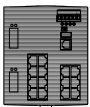





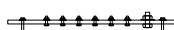
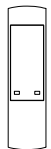
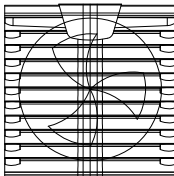
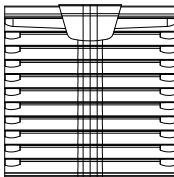
T. +971 (4) 8995000, F. +971 (4) 8995001



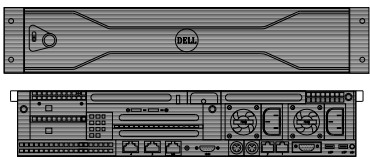
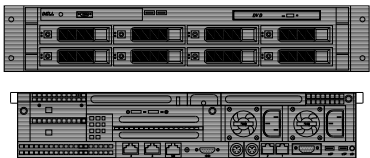
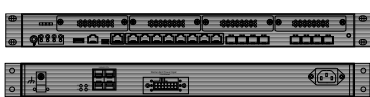





www.silvertech-me.com

STME DWG. NO.	SHEET	REV.
PRJ212-PH4-INS-GAD-0001	02 OF 09	3

SCALE:
N.T.S.
SIZE:
A3
REV:
3

SYMBOLS LEGEND:

	MINIATURE CIRCUIT BREAKER
	DOOR SWITCH
	TERMINAL BLOCKS
	ETHERNET TCP/IP MANAGED SWITCH
	POWER SUPPLY UNIT
	REDUNDANCY MODULE
	KVM EXTENDER (CE750)
	CMC III BUS ACCESS
	CMC III PROCESSING UNIT
	PE & IE BAR
	CMC III READER UNITS
	FAN
	FILTER

	CMC III MOUNTING UNITS
	ETHERNET MANAGED SWITCH (EXTREME X440-G2-24t-10GE4)
	WORK STATION
	SERVER
	FIREWALL
	KVM SWITCH WITH MONITOR
	CABLE MANAGEMENT
	1U BLANK PLATE
	COMPACT LIGHT
	POWER DISTRIBUTION UNIT (PDU)

LEGENDS:

CB	: MINIATURE CIRCUIT BREAKER
DS	: DOOR SWITCH
ES	: ETHERNET SWITCH (EXTREME B5)
LT	: PANEL LIGHT
PDU	: POWER DISTRIBUTION UNIT
SE	: SAFETY EARTH
IE	: INSTRUMENT EARTH
TB	: TERMINAL BLOCKS
OWS	: OPERATOR WORKSTATION SERVER
EWS	: ENGINEERING WORKSTATION SERVER
PU	: PROCESSING UNITS
RU	: READER UNIT
BA	: BUS ACCESS
CT	: CABLE TRAY

NAMING CONVENTION:


RAIL:



REFERENCE DRAWINGS/DOCUMENTS:

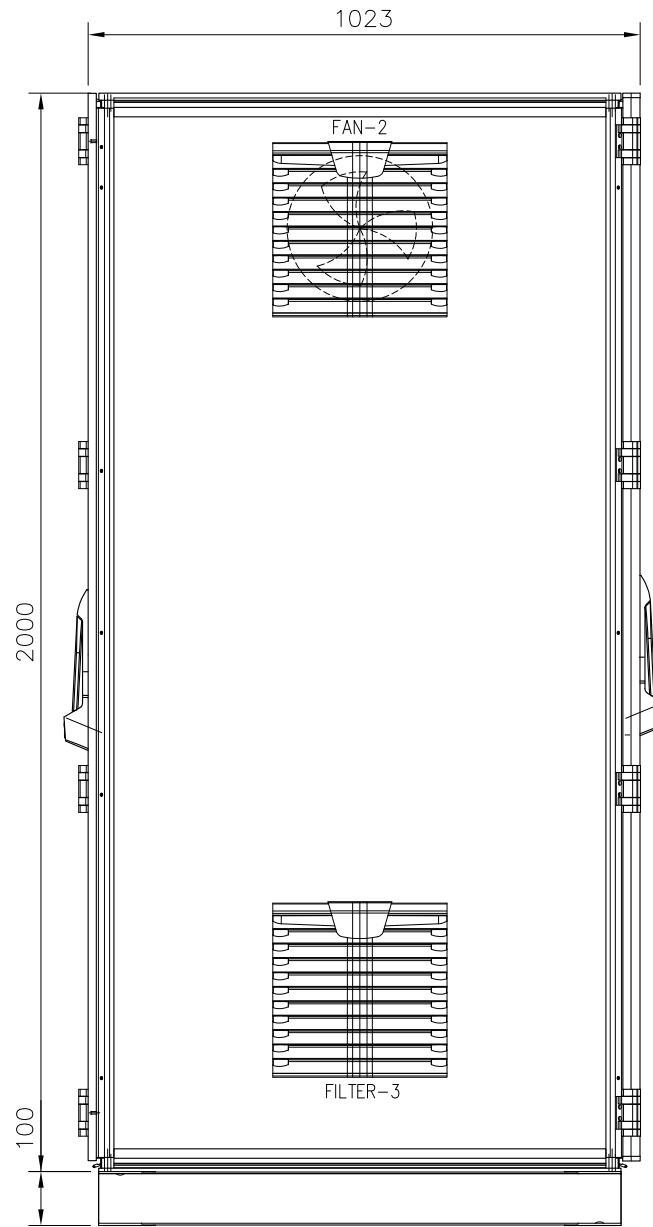
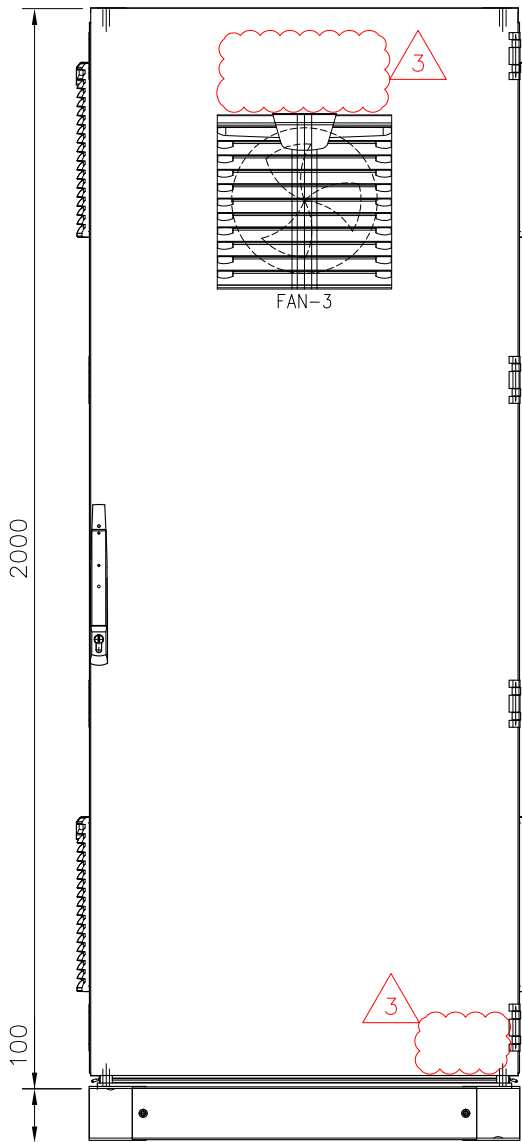
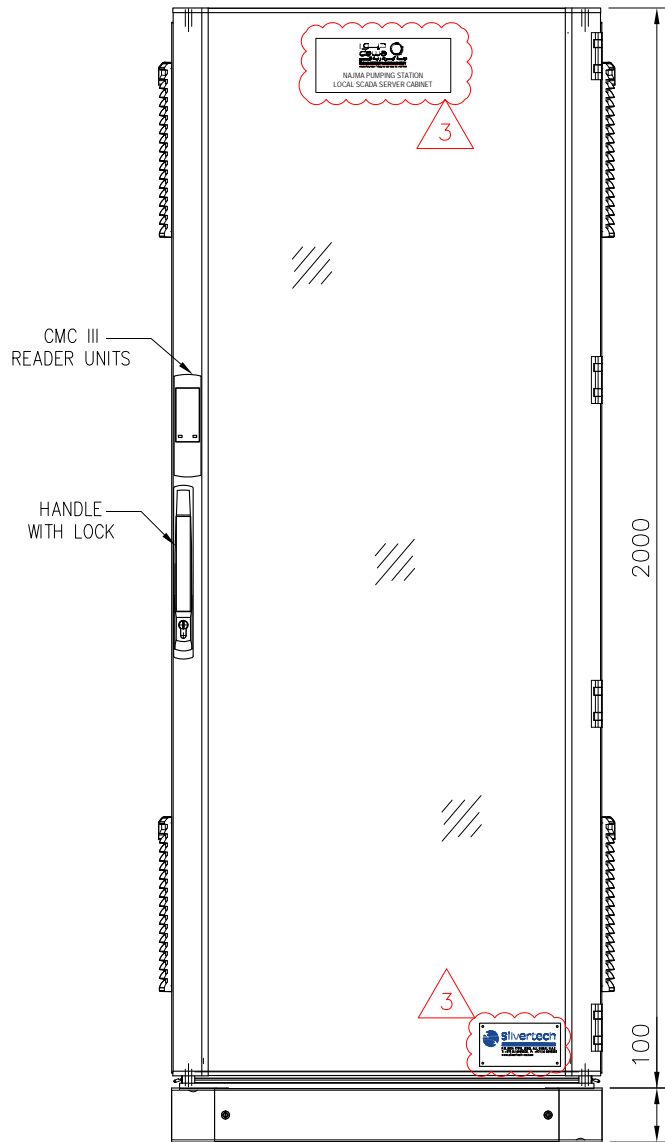
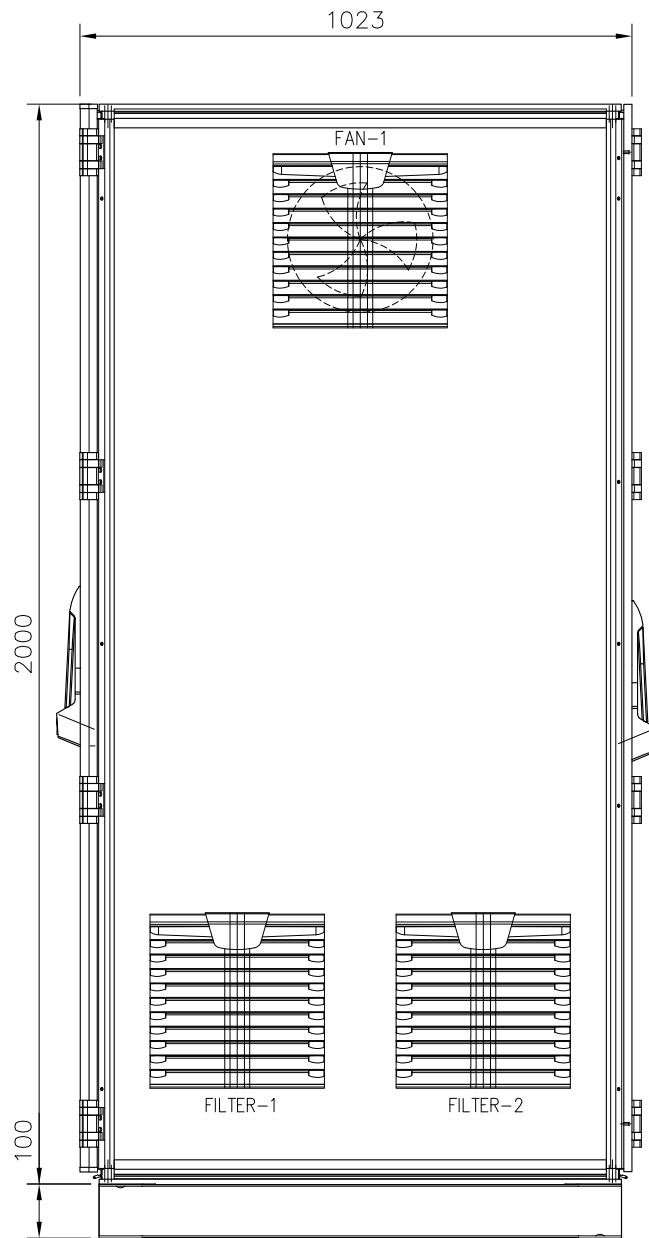
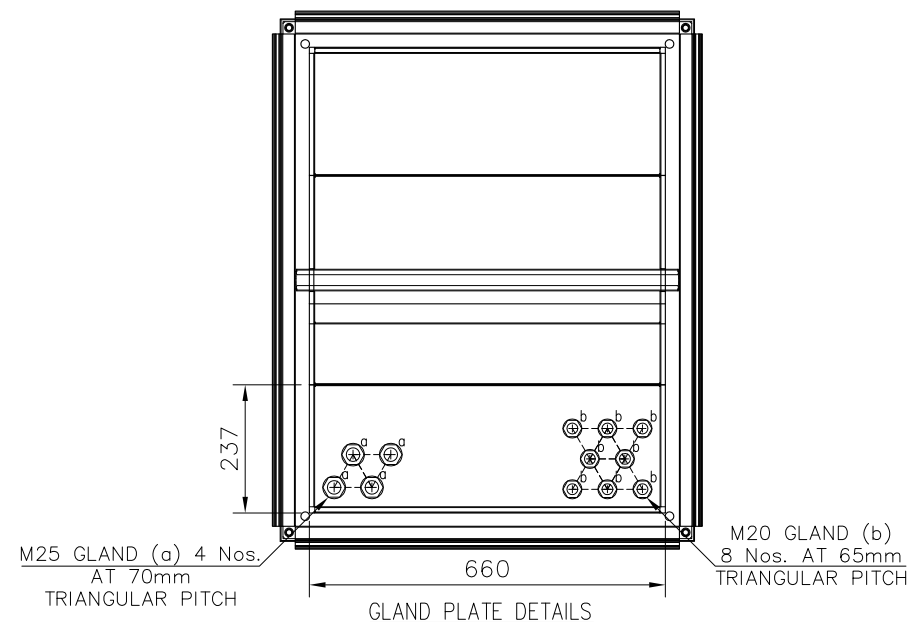
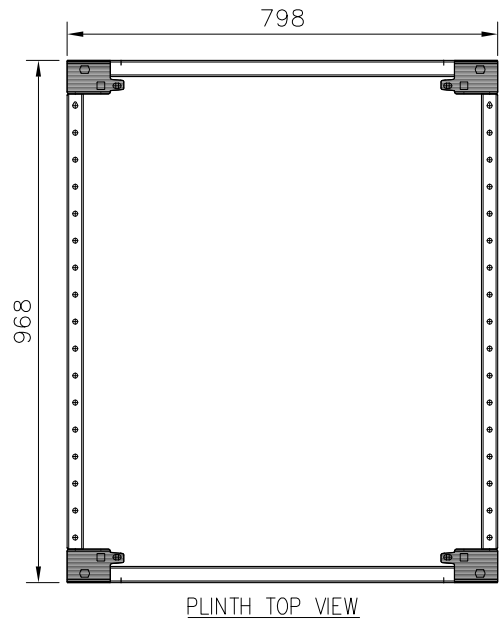
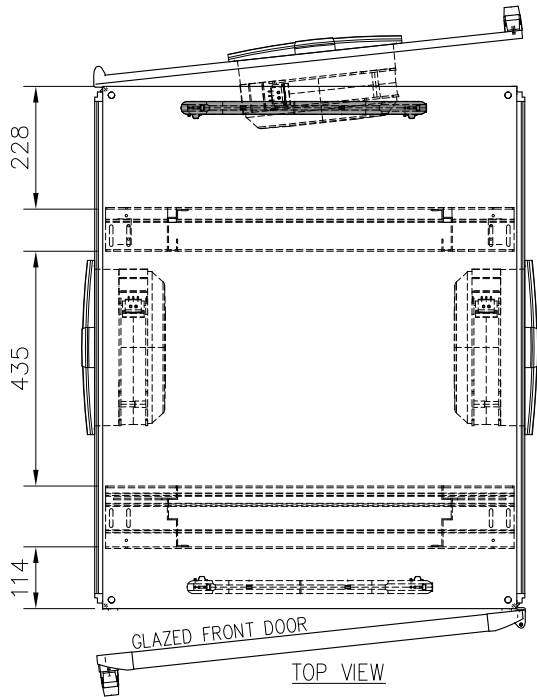
ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD
3	20.07.18	APPROVED FOR CONSTRUCTION	SJM	PLP	NH	AA
2	19.04.18	RE-ISSUED FOR APPROVAL	SJM	JLK	NH	AA
1	11.04.18	ISSUED FOR APPROVAL	SJM	JLK	NH	AA
0	15.02.18	ISSUED FOR REVIEW	SAA	JLK	NH	AA

CLIENT	 هيئة كهرباء ومياه دبي Dubai Electricity & Water Authority	DEWA PRJ REF : RFX-2131600072 DEWA PO REF : PO: 3761700080 DEWA DWG. NO. RFX72-SRV-GAD4
PROJECT:	SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX - PHASE-4 SERVER PANEL GA DRAWING - LEGEND SHEET	

VENDOR	 P.O. BOX: 17910, JEBEL ALI, DUBAI, U.A.E T: +971 (4) 8995000, F: +971 (4) 8995001 www.silvertech-me.com	SCALE: N.T.S.
STME DWG. NO.	PRJ212-PH4-INS-GAD-0001	SIZE: A3
SHEET	03 OF 09	REV: 3

NOTES:

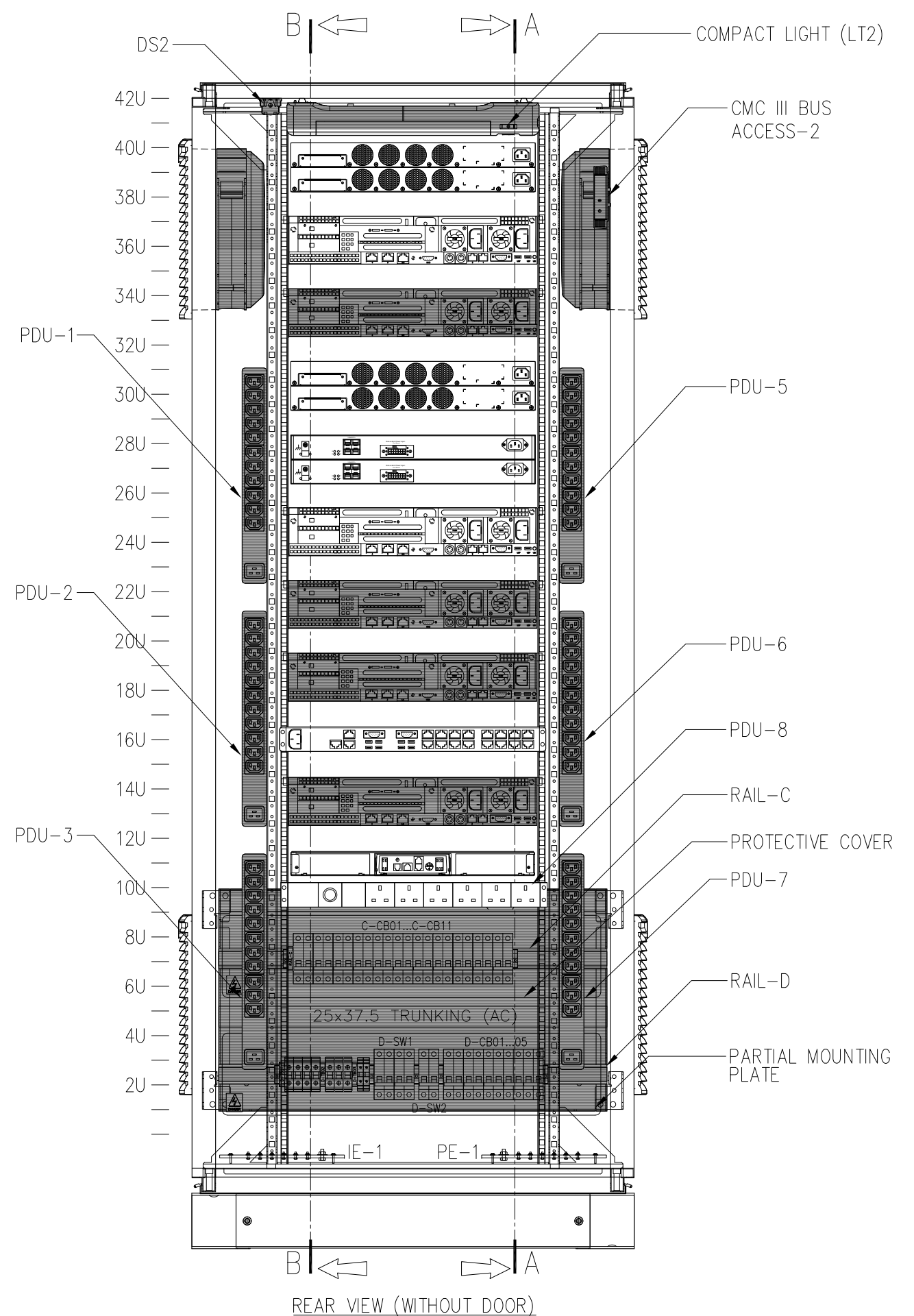
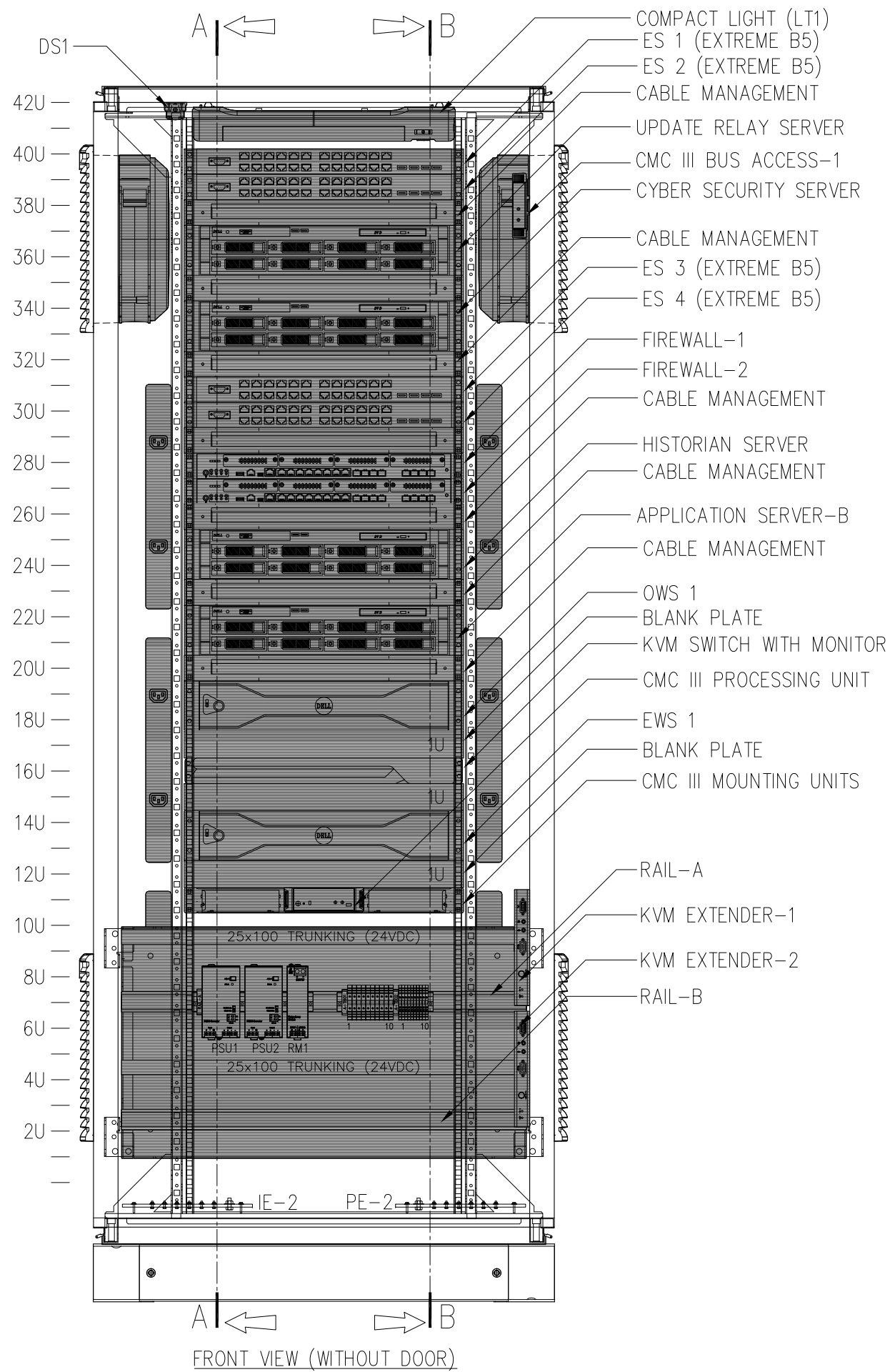
1. RITTAL ENCLOSURE: TS SERIES (WITH FRONT AND REAR DOOR)
DOOR:
FRONT: GLAZED ALUMINIUM DOOR, 180° HINGES
REAR: SHEET STEEL DOOR, 180° HINGES
2. FINISH : RAL 7035
MOUNTING PLATE: ZINC-PLATED
INTERIOR INSTALLATION: RAL 9005
3. CABLE ENTRY IS THROUGH THE BOTTOM OF THE ENCLOSURE.
4. PANEL IS FRONT AND REAR ACCESS
5. ESTIMATED WEIGHT : - 450KG.(APPROX)
6. ALL DIMENSIONS ARE IN "mm"



REFERENCE DRAWINGS/DOCUMENTS:

3	20.07.18	APPROVED FOR CONSTRUCTION	SJM	PLP	NH	AA
2	19.04.18	RE-ISSUED FOR APPROVAL	SJM	JLK	NH	AA
1	11.04.18	ISSUED FOR APPROVAL	SJM	JLK	NH	AA
0	15.02.18	ISSUED FOR REVIEW	SAA	JLK	NH	AA
ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD

CLIENT	DEWA PRJ REF : RFX-2131600072 DEWA PO REF : PO: 3761700080 DEWA DWG. NO. RFX72-SRV-GAD4	VENDOR	SCALE: 1:15 SIZE: A3
PROJECT: SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX - PHASE-4 SERVER PANEL GA DRAWING		STME DWG. NO. PRJ212-PH4-INS-GAD-0001	SHEET 04 OF 09 REV. 3



REFERENCE DRAWINGS/DOCUMENTS:

3	20.07.18	APPROVED FOR CONSTRUCTION	SJM	PLP	NH	AA
2	19.04.18	RE-ISSUED FOR APPROVAL	SJM	JLK	NH	AA
1	11.04.18	ISSUED FOR APPROVAL	SJM	JLK	NH	AA
0	15.02.18	ISSUED FOR REVIEW	SAA	JLK	NH	AA
ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD

CLIENT

هيئة كهرباء ومياه دبي
Dubai Electricity & Water Authority

P.O. BOX: 564, DUBAI, UAE. TEL: 00971-4-324 4444. FAX: 00971-4-324 4922

PROJECT:

SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA
SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY
IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX - PHASE-4 SERVER PANEL GA DRAWING

DEWA PRJ REF : RFX-2131600072

DEWA PO REF : PO: 3761700080

DEWA DWG. NO.

RFX72-SRV-GAD4

VENDOR

Silvertech
SILVERTECH MEASUREMENTS & CONTROL

P.O. BOX: 17910, JEBEL ALI, DUBAI, U.A.E
T: +971 (4) 8995000, F: +971 (4) 8995001
www.silvertech-me.com

STME DWG. NO.

PRJ212-PH4-INS-GAD-0001

SHEET

05 OF 09

SCALE:

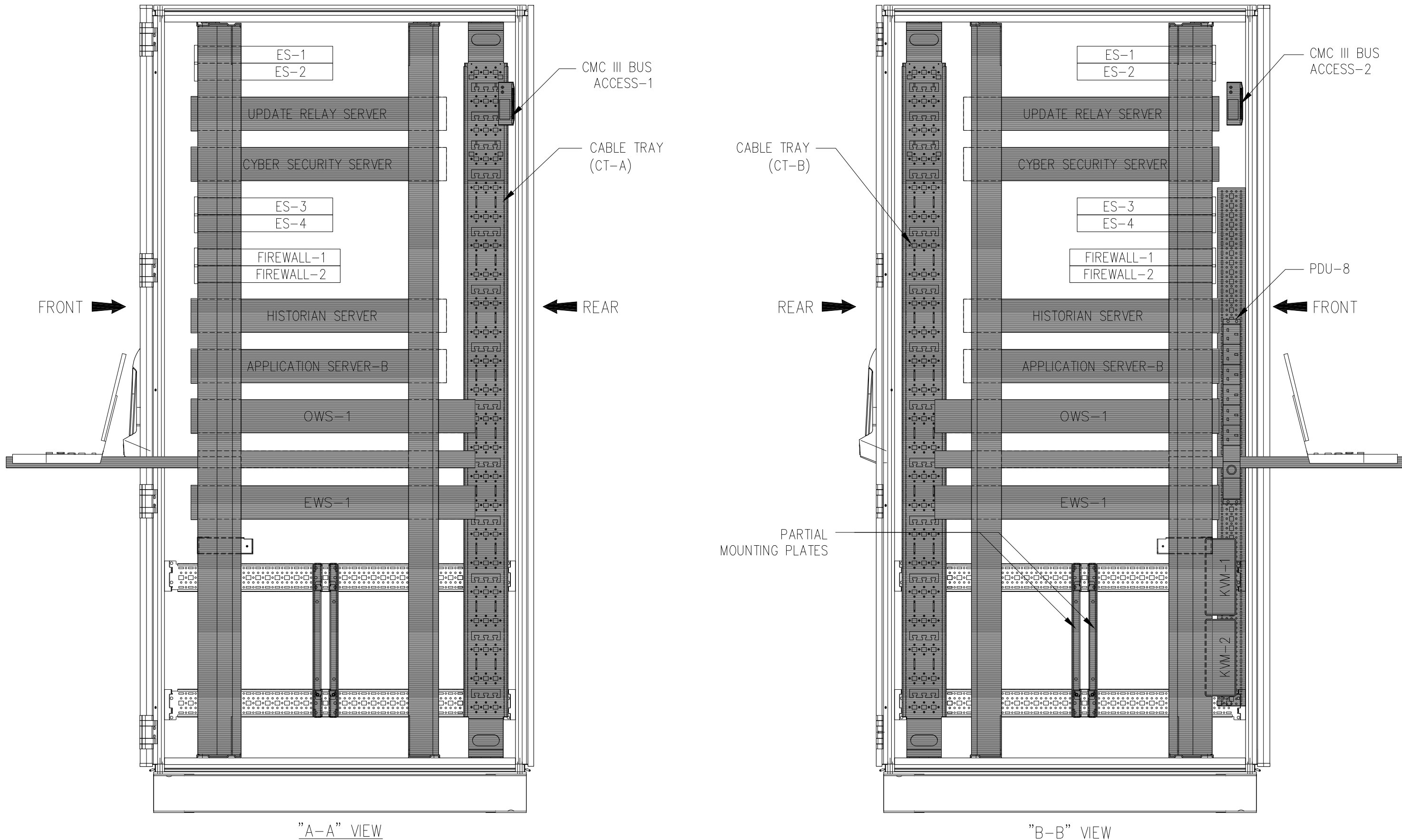
1 : 10

SIZE:

A3

REV.

3



"A-A" VIEW

"B-B" VIEW

REFERENCE DRAWINGS/DOCUMENTS:

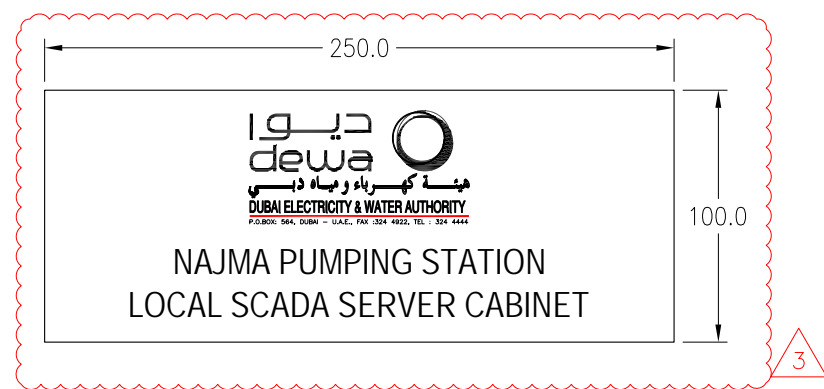
3	20.07.18	APPROVED FOR CONSTRUCTION	SJM	PLP	NH	AA
2	19.04.18	RE-ISSUED FOR APPROVAL	SJM	JLK	NH	AA
1	11.04.18	ISSUED FOR APPROVAL	SJM	JLK	NH	AA
0	15.02.18	ISSUED FOR REVIEW	SAA	JLK	NH	AA
ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD

CLIENT	DEWA PRJ REF : RFX-2131600072 DEWA PO REF : PO: 3761700080 DEWA DWG. NO. RFX72-SRV-GAD4
PROJECT:	SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX - PHASE-4 SERVER PANEL GA DRAWING

VENDOR	SCALE: 1 : 10
SHEET	SIZE: A3
REV: 3	

STME DWG. NO. PRJ212-PH4-INS-GAD-0001	SHEET 06 OF 09
---------------------------------------	----------------

ENCLOSURE LABEL



MATERIAL : STAINLESS STEEL 316L 1.6mm
LABEL : COLOR LASER PRINTED AND LAMINATED
TEXT HEIGHT : 10mm.

LABEL LOCATION : OUTSIDE
FIXING TYPE : ADHESIVE
TEXT FONT : ARIAL

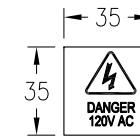
MANUFACTURER LABEL



MATERIAL : STAINLESS STEEL 316L 1.6mm
LABEL : ENGRAVED, INK FILLED AND LAMINATED
TEXT COLOR : BLACK

LABEL LOCATION : OUTSIDE
FIXING TYPE : ADHESIVE

WARNING LABEL

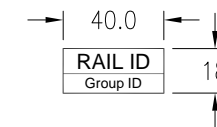


LABEL BACKGROUND : YELLOW
TEXT COLOR : BLACK
TEXT HEIGHT : 4mm.

LABEL LOCATION : INSIDE
FIXING TYPE : ADHESIVE

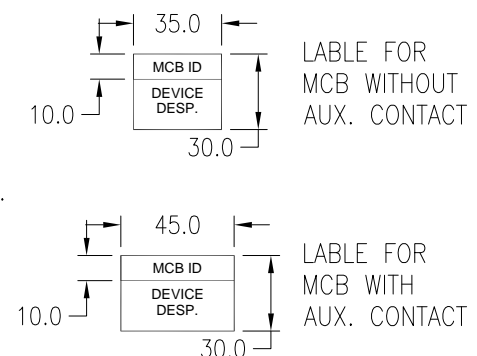
TYPICAL TERMINAL GROUP MARKER

LABEL BACKGROUND : WHITE
TEXT COLOR : BLACK
TEXT HEIGHT 1ST LINE : 6mm.
TEXT HEIGHT 2ND LINE : 4mm.
LABEL LOCATION : INSIDE
FIXING TYPE : ADHESIVE



TYPICAL MCB LABEL

LABEL BACKGROUND : WHITE
TEXT COLOR : BLACK
TEXT HEIGHT 1ST LINE : 4mm.
TEXT HEIGHT 2ND LINE : 4mm.
LABEL LOCATION : INSIDE
FIXING TYPE : ADHESIVE



REFERENCE DRAWINGS/DOCUMENTS:

ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD
3	20.07.18	APPROVED FOR CONSTRUCTION	SJM	PLP	NH	AA
2	19.04.18	RE-ISSUED FOR APPROVAL	SJM	JLK	NH	AA
1	11.04.18	ISSUED FOR APPROVAL	SJM	JLK	NH	AA
0	15.02.18	ISSUED FOR REVIEW	SAA	JLK	NH	AA

CLIENT	DEWA PRJ REF : RFX-2131600072 DEWA PO REF : PO: 3761700080 DEWA DWG. NO. RFX72-SRV-GAD4
PROJECT:	SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX - PHASE-4 SERVER PANEL GA DRAWING-LABEL DETAILS

VENDOR	 P.O. BOX: 17910, JEBEL ALI, DUBAI, U.A.E T: +971 (4) 8995000, F: +971 (4) 8995001 www.silvertech-me.com
--------	--

STME DWG. NO. PRJ212-PH4-INS-GAD-0001	SHEET 07 OF 09	REV. 3
--	-------------------	-----------

SCALE:
N.T.S.

SIZE:
A3

SR NO.	TAGS	DESCRIPTION	MANUFACTURER	PART No.	QTY.
1	-	ENCLOSURE (800W X 1000D X 2000H) WITH FRONT GLAZED DOOR & REAR STEEL DOOR	RITTAL	DK 5509.131	01 No.
2	FAN1....FAN3	FAN	RITTAL	SK 3244.100	03 Nos.
3					
4	-	FILTER	RITTAL	SK 3243.200	4 Nos.
5	LT1, LT2	COMPACT LIGHT	RITTAL	SZ 4140.010	02 Nos.
6	DS1, DS2	DOOR SWITCH	RITTAL	SZ 4127.010	02 Nos.
7	-	FRONT & REAR PANEL (PLINTH)	RITTAL	TS 8601.805	1 SET
8	-	PANEL PLINTH	RITTAL	TS 8601.015	1 SET
9	-	HANDLE WITH SEMI CYLINDER	RITTAL	DK 7320.721 + SZ 2467.000	02 Nos.
10	RU-1	CMC III READER UNITS	RITTAL	DK 7030.230	01 No.
11	-	UPDATE RELAY SERVER (2U FORM FACTOR)	DELL	POWER EDGE R530	01 No.
12	-	CYBER SECURITY SERVER (2U FORM FACTOR)	DELL	POWER EDGE R530	01 No.
13	ES 1 - ES 4	MANAGED ETHERNET SWITCH	EXTREME	X440-G2-24t-10GE4	04 Nos.
14	-	HISTORIAN SERVER (2U FORM FACTOR)	DELL	POWER EDGE R530	01 No.
15	-	APPLICATION SERVER-B (2U FORM FACTOR)	DELL	POWER EDGE R530	01 No.
16	-	FIREWALL	JUNIPER	SRX340	02 Nos.
17	OWS 1	OPERATOR WORKSTATION SERVER (2U FORM FACTOR)	DELL	PRECISION 7910	01 No.
18	-	DAV2216-G01 KVM SWITCH + 1U RACKMOUNT LED CONSOLE	DELL	A7485896 + FPM185	01 No.
19	EWS 1	ENGINEERING WORKSTATION SERVER (2U FORM FACTOR)	DELL	PRECISION 7910	01 No.
20	PU-1	CMC III PROCESSING UNITS	RITTAL	DK 7030.010	01 No.
21	-	CMC III MOUNTING UNIT	RITTAL	DK 7030.070	01 No.
22	-	1U 19" BLANK PLATE	RITTAL	DK 7151.005	03 Nos.
23	-	19" CABLE MANAGEMENT PANEL WITH BRUSH STRIP	RITTAL	DK-5502.265	07 Nos.
24	KVM1 - KVM2	KVM EXTENDER	ATEN	CE750	02 Nos.
25	BA-1 & BA-2	CMC III CAN BUS ACCESS	RITTAL	DK 7030.200	02 Nos.
		RAIL-A			
26	PSU1 & PSU2	POWER SUPPLY 200V-240V AC/24V 28V DC 20A	PULS	CPS20.241-C1	02 Nos.
27	RM1	DUAL REDUNDANCY MODULE 12-28V, 40A	PULS	YR40.242	01 No.
28	A-TB1	FUSE TERMINAL (WSI 6)	WEIDMULLER	1011000000	10 Nos.
29	A-TB2	FEED THROUGH TERMINAL (WDU 4)	WEIDMULLER	1020100000	10 Nos.
		RAIL-B			
30	-	SPARE RAIL	-	-	-
		RAIL-C			
31	C-CB1	MCB 16A 2P	SCHNEIDER ELECTRIC	A9F44216	01 No.
32	C-CB2 - C-CB4	MCB 10A 2P	SCHNEIDER ELECTRIC	A9F44210	03 Nos.
33	C-CB5 - C-CB8	MCB 4A 2P	SCHNEIDER ELECTRIC	A9F44204	04 Nos.

REFERENCE DRAWINGS/DOCUMENTS:

3	20.07.18	APPROVED FOR CONSTRUCTION	SJM	PLP	NH	AA	
2	19.04.18	RE-ISSUED FOR APPROVAL	SJM	JLK	NH	AA	
1	11.04.18	ISSUED FOR APPROVAL	SJM	JLK	NH	AA	
0	15.02.18	ISSUED FOR REVIEW	SAA	JLK	NH	AA	
ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD	

CLIENT

هيئة كهرباء ومياه دبي

Dubai Electricity & Water Authority




P.O. BOX: 564, DUBAI, UAE TEL: 00971-4-324 4444 FAX: 00971-4-324 4922

DEWA PRJ REF : RFX-2131600072
DEWA PO REF : PO: 3761700080
DEWA DWG. NO.
RFX72-SRV-GAD4

PROJECT:
SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA
SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY
IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX - PHASE-4 SERVER PANEL BOM

VENDOR



Silvertech

Authorised Supplier of SCADA Systems

P.O. BOX: 17910, JEBEL ALI, DUBAI, U.A.E
T. +971 (4) 8995000, F. +971 (4) 8995001
www.silvertech-me.com

STME DWG. NO.
PRJ212-PH4-INS-GAD-0001

SHEET
08 OF 09


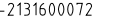
REV.
3

SCALE:
N.T.S.

SIZE:
A3

REV.
3

[illegible]

REFERENCE DRAWINGS/DOCUMENTS:								<div>CLIENT</div> <div><div><div>هيئة كهرباء ومياه دبي</div><div>Dubai Electricity & Water Authority</div></div><div></div><div>DEWA PRJ REF : RFX-2131600072 DEWA PO REF : PO: 3761700080 DEWA DWG. NO. RFX72-SRV-GAD4</div></div> <div>P.O. BOX 564, DUBAI, UAE. TEL. 00971-4-324 4444. FAX. 00971-4-324 4922</div> <div>PROJECT: SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX - PHASE-4 SERVER PANEL BOM</div>	<div>VENDOR</div> <div><div><div>Silvertech</div><div>PO BOX 17910, JEBEL ALI, DUBAI, U.A.E T. +971 (4) 8995000, F. +971 (4) 8995001 www.silvertech-me.com</div></div></div> <div>STME DWG. NO. PRJ212-PH4-INS-GAD-0001</div> <div>SHEET 09 OF 09</div>		SCALE: N.T.S. SIZE: A3 REV.: 3
	3	20.07.18	APPROVED FOR CONSTRUCTION	SJM	PLP	NH	AA				
	2	19.04.18	RE-ISSUED FOR APPROVAL	SJM	JLK	NH	AA				
	1	11.04.18	ISSUED FOR APPROVAL	SJM	JLK	NH	AA				
	0	15.02.18	ISSUED FOR REVIEW	SAA	JLK	NH	AA				
	ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD				

SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX

GENERAL ARRANGEMENT DRAWING
PHASE-1 PLC PANEL

REFERENCE DRAWINGS/DOCUMENTS:

2	06.05.18	ISSUED FOR CONSTRUCTION	SJM	JLK	NH	AA	
1	03.04.18	ISSUED FOR APPROVAL	SJM	JLK	NH	AA	
0	12.02.18	ISSUED FOR REVIEW	SAA	JLK	NH	AA	
ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD	

CLIENT

هيئة كهرباء ومياه دبي

Dubai Electricity & Water Authority

P.O. BOX: 564, DUBAI, UAE. TEL: 00971-4-324 4444. FAX: 00971-4-324 4922

DEWA PRJ REF : RFX-2131600072

DEWA PO REF : PO: 3761700080


DEWA DWG. NO.

RFX72-PLC-GAD1

PROJECT:

SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX - PHASE-1 PLC PANEL GA DRAWING - COVER SHEET

VENDOR



Silvertech

P.O. BOX: 17910, JEBEL ALI, DUBAI, U.A.E
T: +971 (4) 8995000, F: +971 (4) 8995001
www.silvertech-me.com

SCALE:

N.T.S.

SIZE:

A3

REV.

2

STME DWG. NO.

PRJ212-PH1-INS-GAD-0001

SHEET

01 OF 10

PRJ212-PH1-INS-GAD-0001-02

SHEET NO.	DESCRIPTION	FILE NAME	ISSUE	REVISIONS				PURPOSE OF ISSUE
				0	1	2	3	
1	PHASE-1 PLC PANEL GENERAL ARRANGEMENT DRAWING - COVER SHEET	PRJ212-PH1-INS-GAD-0001-01	06.05.18	X	X	X		ISSUED FOR CONSTRUCTION
2	PHASE-1 PLC PANEL GENERAL ARRANGEMENT DRAWING - INDEX SHEET	PRJ212-PH1-INS-GAD-0001-02	06.05.18	X	X	X		ISSUED FOR CONSTRUCTION
3	PHASE-1 PLC PANEL GENERAL ARRANGEMENT DRAWING	PRJ212-PH1-INS-GAD-0001-03	06.05.18	X	X	X		ISSUED FOR CONSTRUCTION
4	PHASE-1 PLC PANEL GENERAL ARRANGEMENT DRAWING	PRJ212-PH1-INS-GAD-0001-04	06.05.18	X	X	X		ISSUED FOR CONSTRUCTION
5	PHASE-1 PLC PANEL GENERAL ARRANGEMENT DRAWING	PRJ212-PH1-INS-GAD-0001-05	06.05.18	X	X	X		ISSUED FOR CONSTRUCTION
6	PHASE-1 PLC PANEL GENERAL ARRANGEMENT DRAWING - RACK DETAILS	PRJ212-PH1-INS-GAD-0001-06	06.05.18	X	X	X		ISSUED FOR CONSTRUCTION
7	PHASE-1 PLC PANEL GENERAL ARRANGEMENT DRAWING - BILL OF MATERIAL	PRJ212-PH1-INS-GAD-0001-07	06.05.18	X	X	X		ISSUED FOR CONSTRUCTION
8	PHASE-1 PLC PANEL GENERAL ARRANGEMENT DRAWING - BILL OF MATERIAL	PRJ212-PH1-INS-GAD-0001-08	06.05.18	X	X	X		ISSUED FOR CONSTRUCTION
9	PHASE-1 PLC PANEL GENERAL ARRANGEMENT DRAWING - BILL OF MATERIAL	PRJ212-PH1-INS-GAD-0001-09	06.05.18	X	X	X		ISSUED FOR CONSTRUCTION
10	PHASE-1 PLC PANEL GENERAL ARRANGEMENT DRAWING - BILL OF MATERIAL	PRJ212-PH1-INS-GAD-0001-10	06.05.18	X	X	X		ISSUED FOR CONSTRUCTION
11								
12								
13								
14								
15								
16								
17								
18								
19								
20								
21								
22								
23								
24								
25								
26								
27								
28								
29								
30								
31								
32								
33								
34								
35								
36								
37								
38								

REFERENCE DRAWINGS/DOCUMENTS:

2	06.05.18	ISSUED FOR CONSTRUCTION	SJM	JLK	NH	AA	
1	03.04.18	ISSUED FOR APPROVAL	SJM	JLK	NH	AA	
0	12.02.18	ISSUED FOR REVIEW	SAA	JLK	NH	AA	
ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD	

CLIENT

هيئة كهرباء ومياه دبي

Dubai Electricity & Water Authority

DEWA PRJ REF : RFX-2131600072

DEWA PO REF : PO: 3761700080

DEWA DWG. NO. RFX72-PLC-GAD1

P.O. BOX: 564, DUBAI, UAE. TEL: 00971-4-324 4444. FAX: 00971-4-324 4922

PROJECT: SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX - PHASE-1 PLC PANEL GA DRAWING-INDEX SHEET

VENDOR

Silvertech

P.O. BOX: 17910, JEBEL ALI, DUBAI, U.A.E

T: +971 (4) 8995000. F: +971 (4) 8995001

www.silvertech-me.com

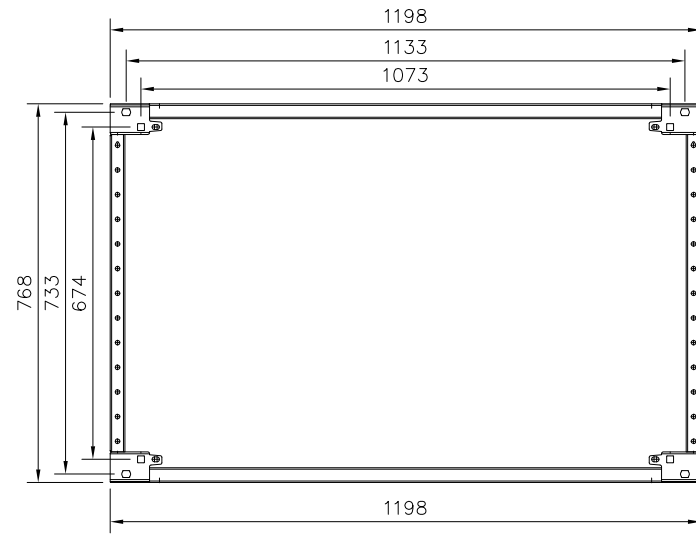
STME DWG. NO. PRJ212-PH1-INS-GAD-0001

SHEET 02 OF 10

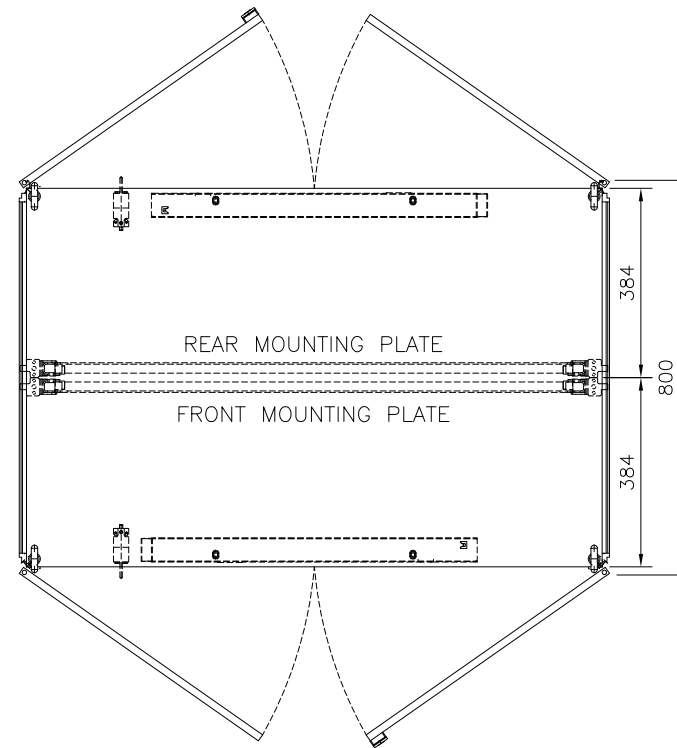
SCALE: N.T.S.

SIZE: A3

REV. 2

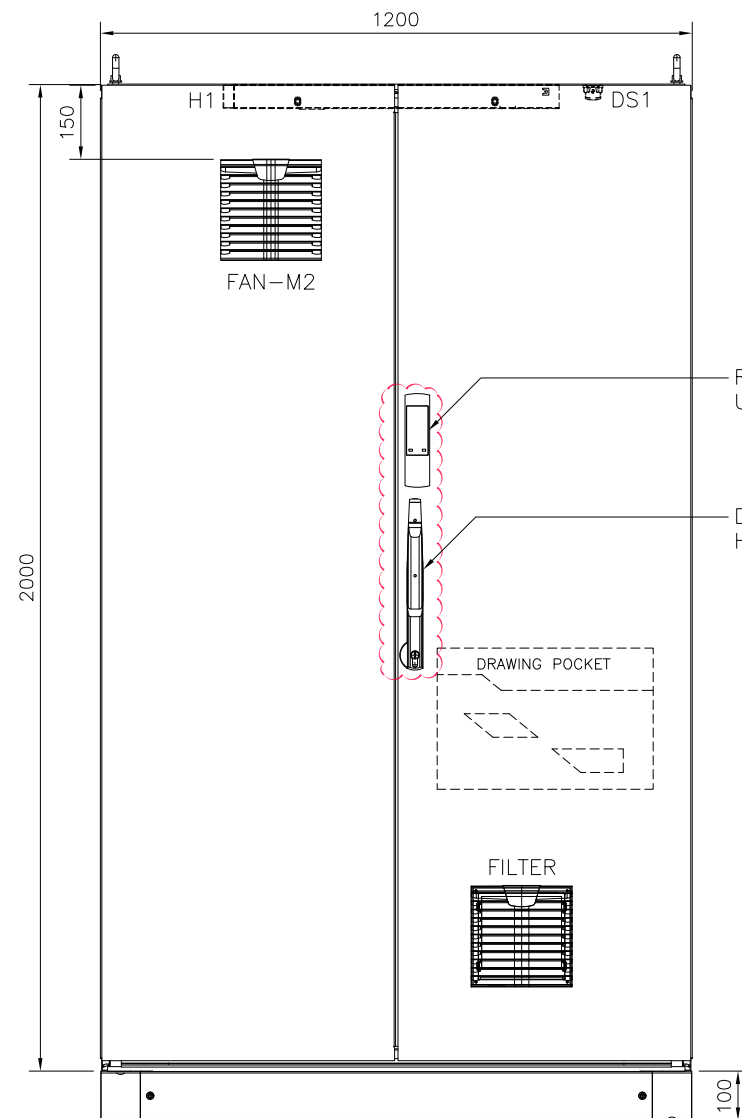


PLINTH TOP VIEW

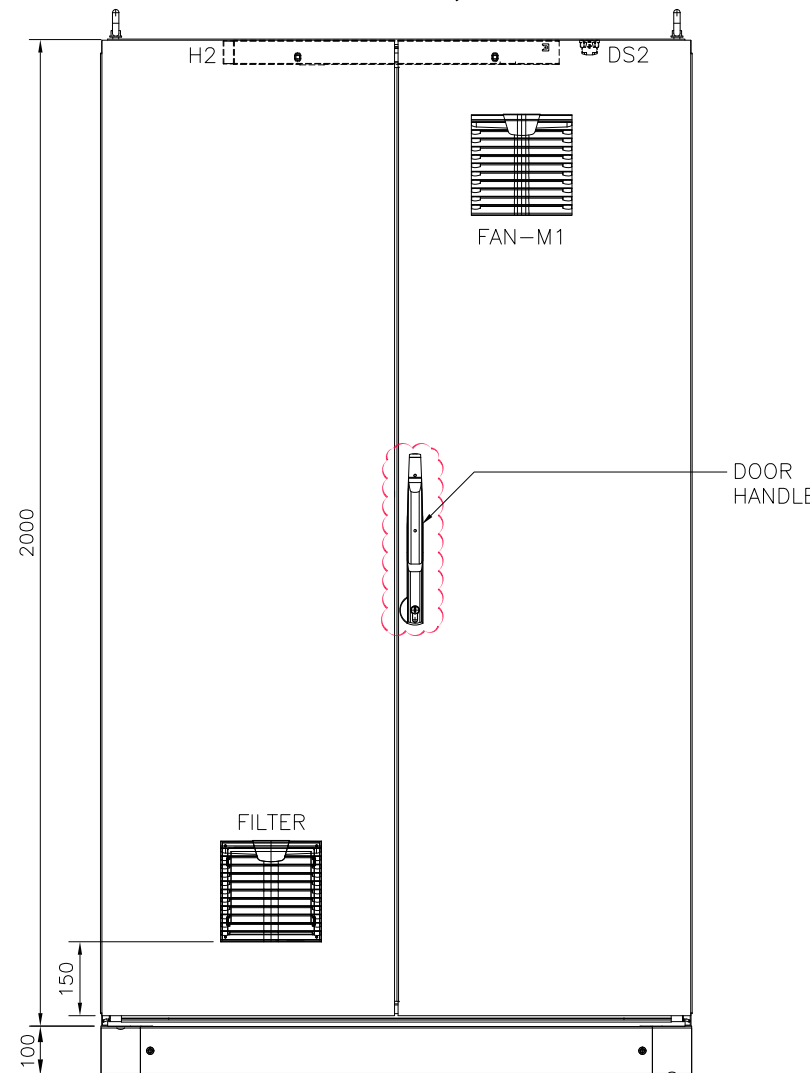


NOTES:

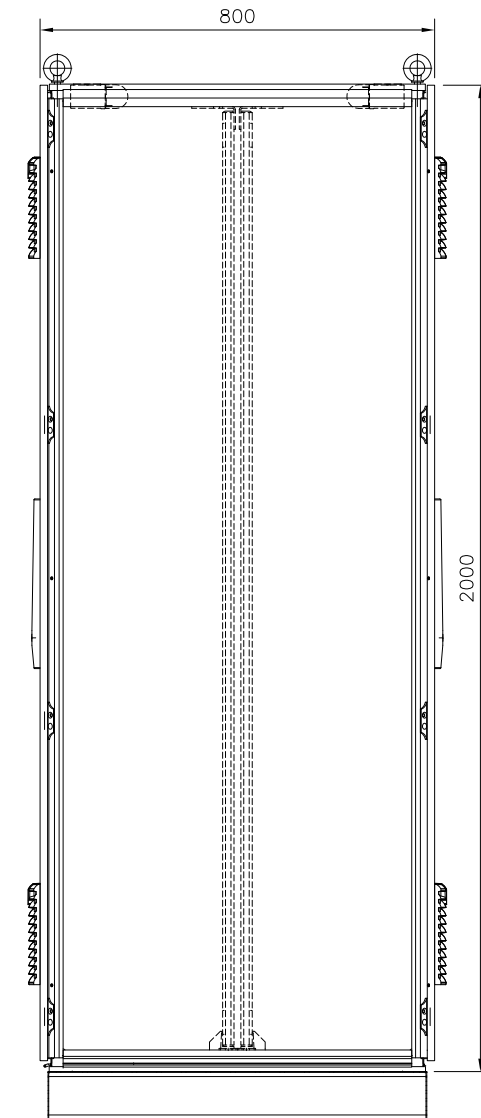
1. RITTAL ENCLOSURE: TS 8208.521 (WITH FRONT AND REAR DOOR)
2. ENCLOSURE FRAME: DIPCOAT PRIMED IN RAL 7035 1.5MM THICK SHEET STEEL.
3. DOORS: DIPCOAT PRIMED AND POWDER AND POWDER COATED IN TEXTURED RAL 7035 2MM THICK SHEET STEEL.
4. ROOF: DIPCOAT PRIMED AND POWDER COATED IN TEXTURED RAL 7035 1.5MM THICK SHEET STEEL.
5. MOUNTING PLATE: ZINC PLATED 3MM THICK SHEET STEEL.
6. PLINTH: RAL 7022 SHEET STEEL.
7. PROTECTION CATEGORY: IP54 TO EN 60529/10.91
8. COMPLIES WITH: NEMA 12
9. CABLE ENTRY & EXIT: BOTTOM.



FRONT VIEW WITH DOOR



REAR VIEW WITH DOOR



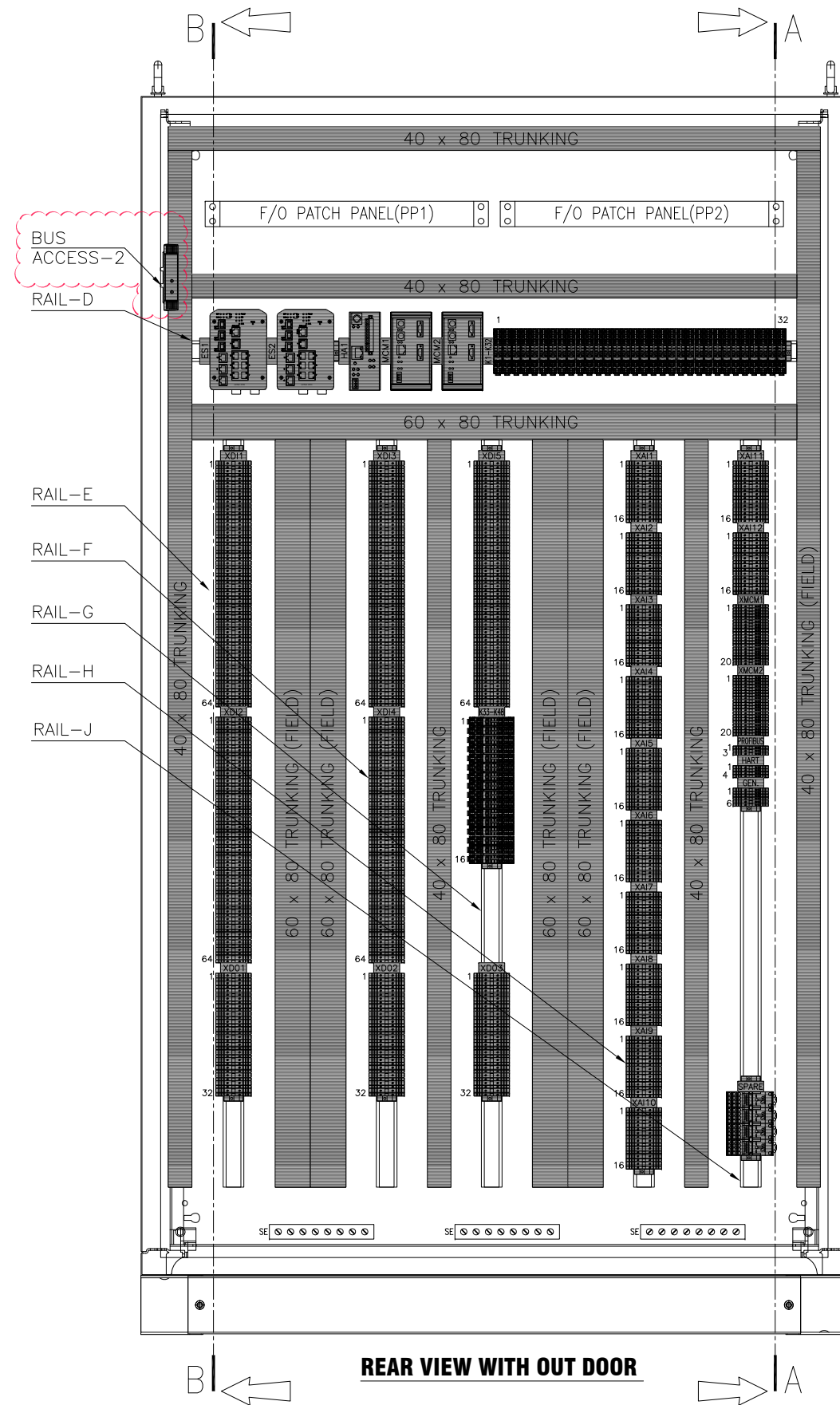
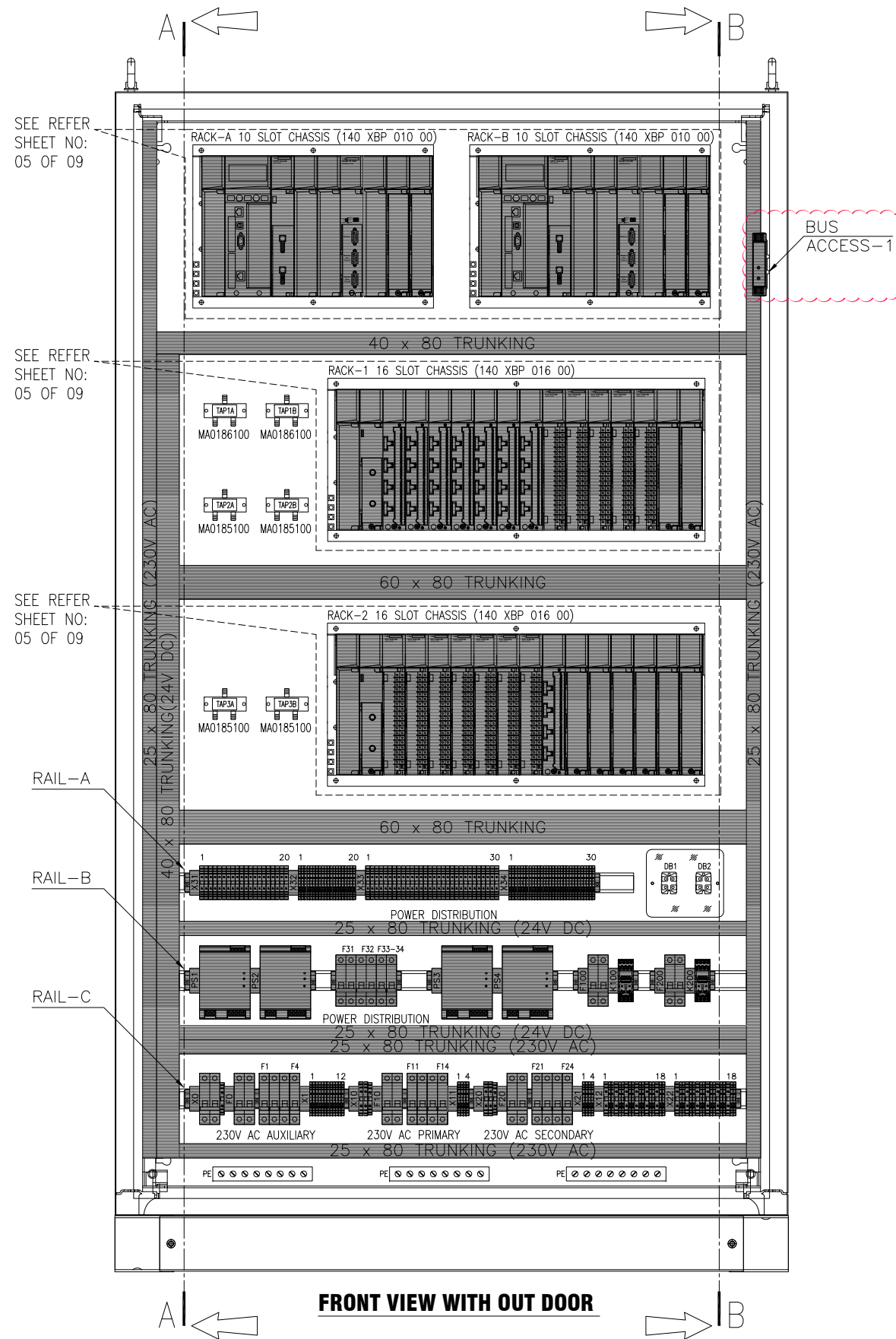
SIDE VIEW

LEGEND:

- CONSTRUCTION SCOPE
- REVISION CLOUD

ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD
2	06.05.18	ISSUED FOR CONSTRUCTION	SJM	JLK	NH	AA
1	03.04.18	ISSUED FOR APPROVAL	SJM	JLK	NH	AA
0	12.02.18	ISSUED FOR REVIEW	SAA	JLK	NH	AA

CLIENT هيئة كهرباء ومياه دبي Dubai Electricity & Water Authority P.O. BOX: 564, DUBAI, UAE. TEL: 00971-4-324 4444. FAX: 00971-4-324 4922	DEWA PRJ REF : RFX-2131600072 DEWA PO REF : PO: 3761700080	VENDOR P.O. BOX: 17910, JEBEL ALI, DUBAI, U.A.E T: +971 (4) 8995000, F: +971 (4) 8995001 www.silvertech-me.com	SCALE: 1 : 15 SIZE: A3
PROJECT: SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX - PHASE-1 PLC PANEL GA DRAWING	DEWA DWG. NO. RFX72-PLC-GAD1	STME DWG. NO. PRJ212-PH1-INS-GAD-0001	SHEET 03 OF 10 REV. 2



LEGEND:

- CONSTRUCTION SCOPE
- REVISION CLOUD

ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD
2	06.05.18	ISSUED FOR CONSTRUCTION	SJM	JLK	NH	AA
1	03.04.18	ISSUED FOR APPROVAL	SJM	JLK	NH	AA
0	12.02.18	ISSUED FOR REVIEW	SAA	JLK	NH	AA

CLIENT

هيئة كهرباء ومياه دبي
Dubai Electricity & Water Authority

P.O. BOX: 564, DUBAI, UAE. TEL: 00971-4-324 4444. FAX: 00971-4-324 4922

PROJECT:

SUPPLY, INSTALLATION, TESTING, COMMISSIONING OF NEW SCADA SYSTEM ALONG WITH PHASE 11 PLC RE-ENGINEERING, NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION - PHASE-1 PLC PANEL GA DRAWING

DEWA PRJ REF : RFX-2131600072

DEWA PO REF : PO: 3761700080

DEWA DWG. NO.
RFX72-PLC-GAD1

VENDOR

Silvertech

P.O. BOX: 17910, JEBEL ALI, DUBAI, U.A.E.
T: +971 (4) 8995000, F: +971 (4) 8995001
www.silvertech-me.com

STME DWG. NO.

PRJ212-PH1-INS-GAD-0001

SHEET

04 OF 10

SCALE:

1 : 10

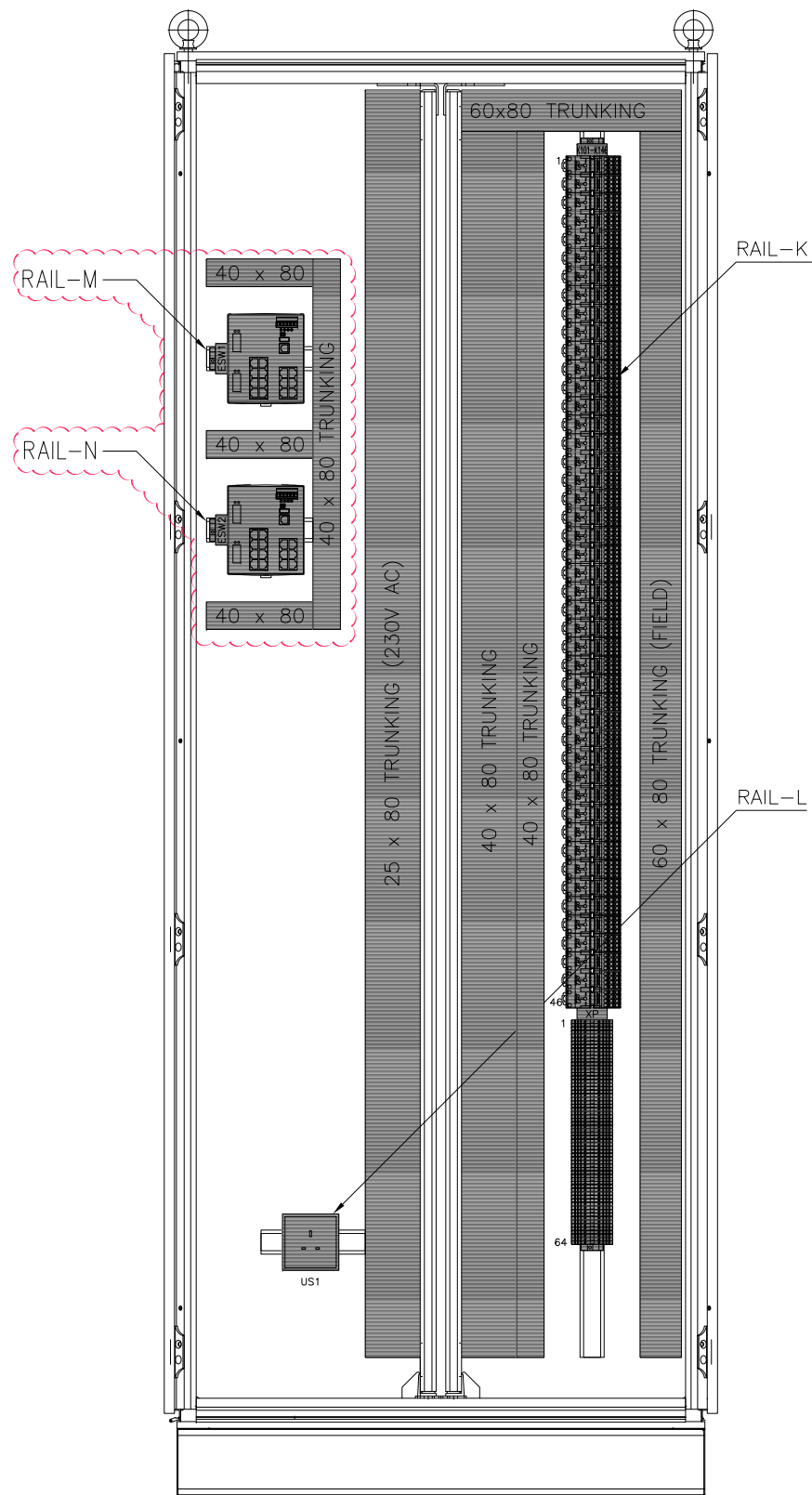
SIZE:

A3

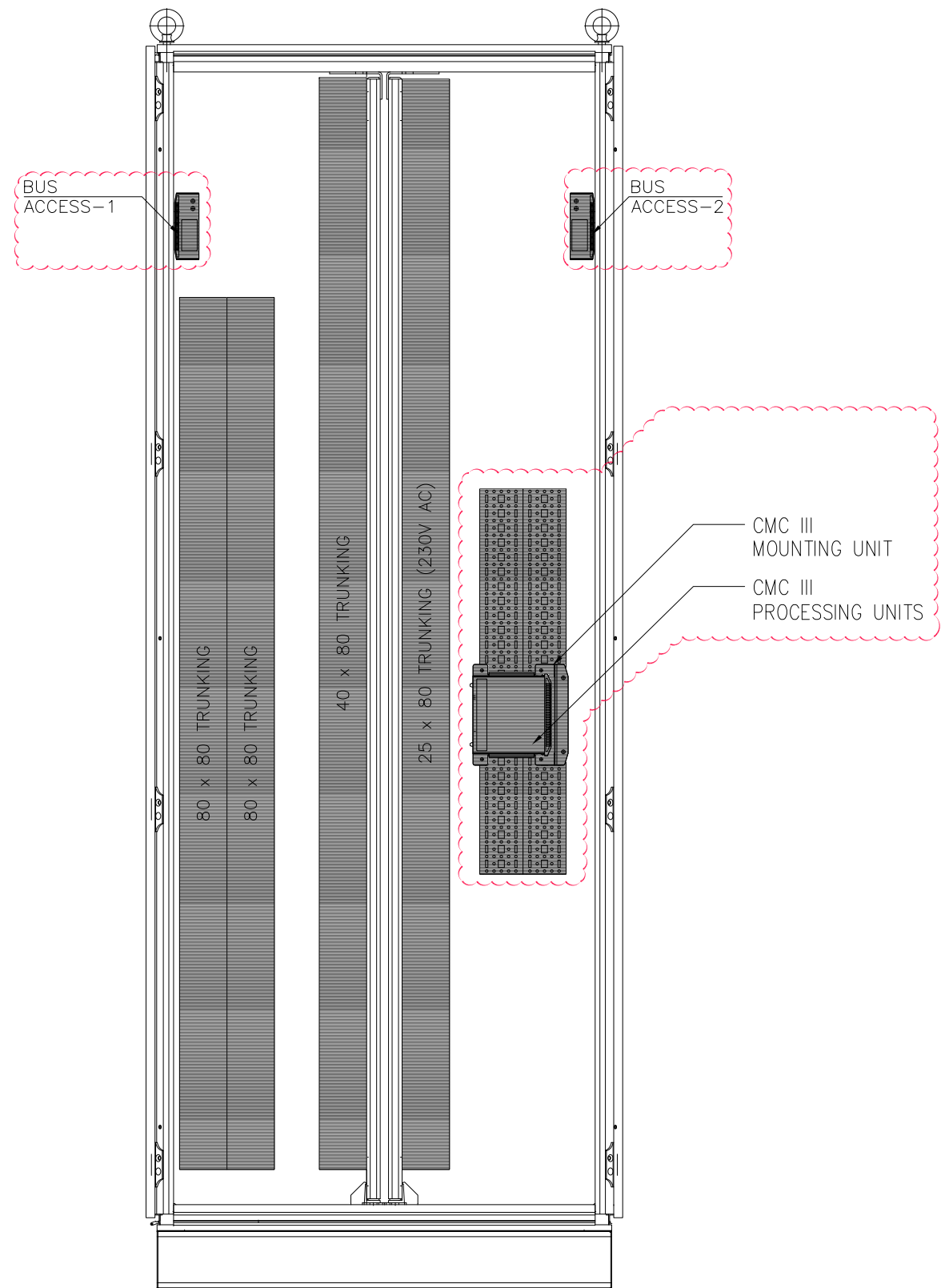
REV.

2

PRJ212-PH1-INS-GAD-0001-05



"A-A" VIEW





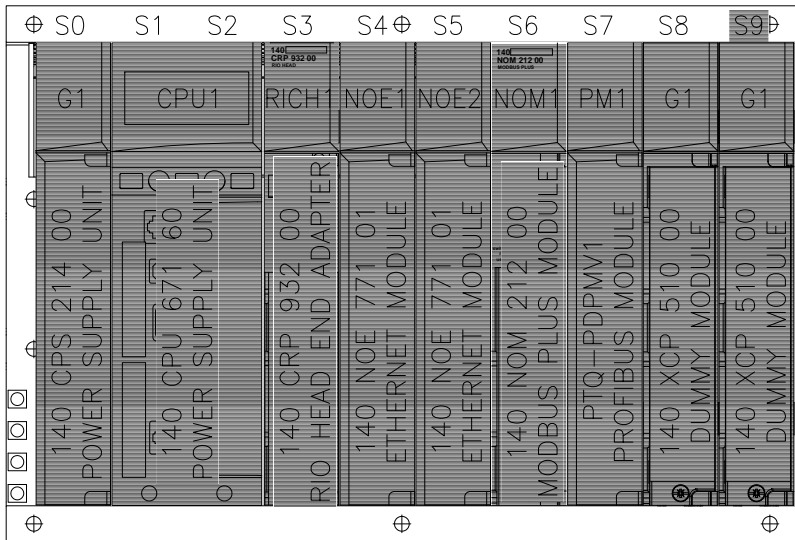
"B-B" VIEW

LEGEND:

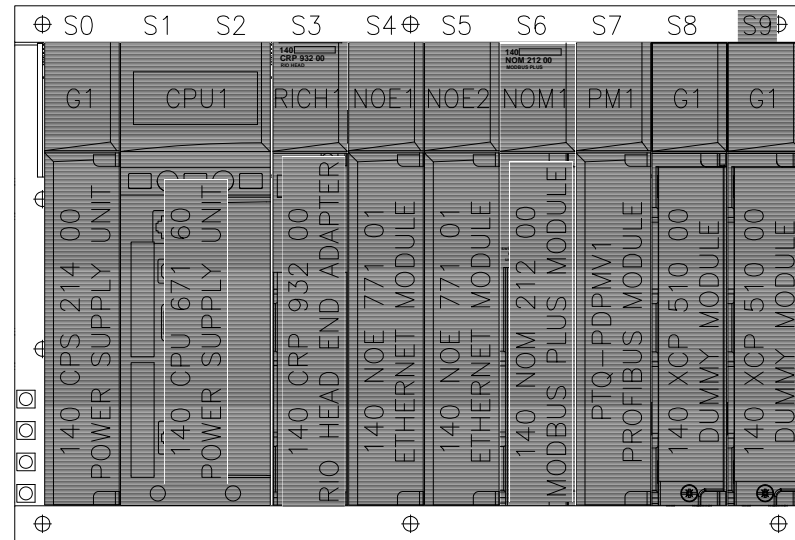
- CONSTRUCTION SCOPE
- REVISION CLOUD

ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD
2	06.05.18	ISSUED FOR CONSTRUCTION	SJM	JLK	NH	AA
1	03.04.18	ISSUED FOR APPROVAL	SJM	JLK	NH	AA
0	12.02.18	ISSUED FOR REVIEW	SAA	JLK	NH	AA

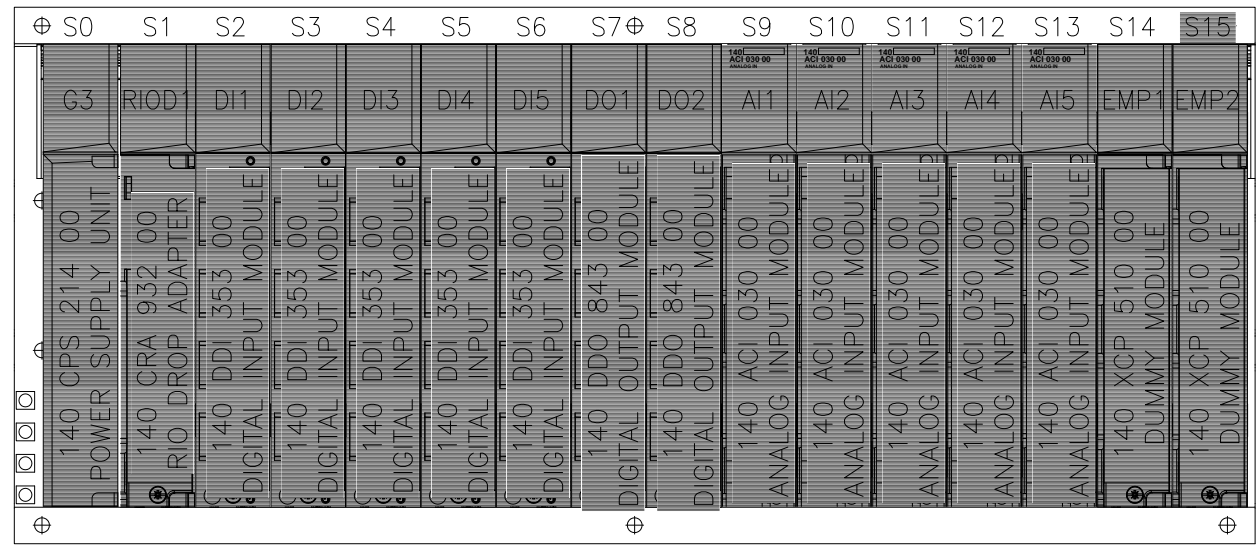
CLIENT	<div><div>هيئة كهرباء ومياه دبي Dubai Electricity & Water Authority</div><div></div></div> <div>P.O. BOX: 564, DUBAI, UAE. TEL: 00971-4-324 4444. FAX: 00971-4-324 4922</div>	DEWA PRJ REF : RFX-2131600072 DEWA PO REF : PO: 3761700080 DEWA DWG. NO. RFX72-PLC-GAD1	VENDOR	<div><div><div>Silvertech</div><div>طاقة - مياه - خدمات</div></div><div>P.O. BOX: 17910, JEBEL ALI, DUBAI, U.A.E T: +971 (4) 8995000, F: +971 (4) 8995001 www.silvertech-me.com</div></div>	SCALE: 1 : 10
PROJECT:	SUPPLY, INSTALLATION, TESTING, COMMISSIONING OF NEW SCADA SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING, NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX - PHASE-1PLC PANEL GA DRAWING	STME DWG. NO. PRJ212-PH1-INS-GAD-0001	SHEET 05 OF 10	SIZE: A3 REV. 2	



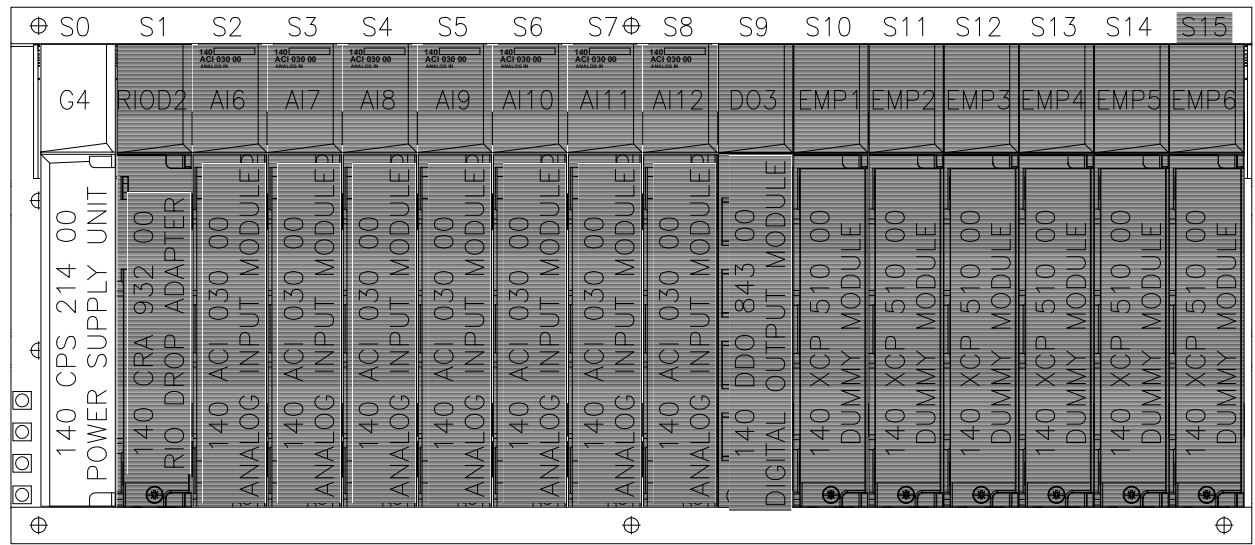
RACK-A 10 SLOT CHASSIS (140 XBP 010 00)



RACK-B 10 SLOT CHASSIS (140 XBP 010 00)



RACK-1 16 SLOT CHASSIS (140 XBP 016 00)




RACK-2 16 SLOT CHASSIS (140 XBP 016 00)

RACK DETAILS

REFERENCE DRAWINGS/DOCUMENTS:

2	06.05.18	ISSUED FOR CONSTRUCTION	SJM	JLK	NH	AA	
1	03.04.18	ISSUED FOR APPROVAL	SJM	JLK	NH	AA	
0	12.02.18	ISSUED FOR REVIEW	SAA	JLK	NH	AA	
ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD	

CLIENT	 P.O. BOX: 564, DUBAI, UAE. TEL: 00971-4-324 4444. FAX: 00971-4-324 4922	DEWA PRJ REF : RFX-2131600072 DEWA PO REF : PO: 3761700080 DEWA DWG. NO. RFX72-PLC-GAD1
PROJECT:	SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX - PHASE-1 PLC PANEL GA DRAWING-RACK DETAILS	



VENDOR	
 <div>Silvertech SPECIALTY MECHANICAL CONTRACTORS</div> <p>P.O. BOX: 17910, JEBEL ALI, DUBAI, U.A.E T: +971 (4) 8995000, F: +971 (4) 8995001 www.silvertech-me.com</p>	
STME DWG. NO.	SHEET
PRJ212-PH1-INS-GAD-0001	06 OF 10

SCALE:	N.T.S.
SIZE:	A3
REV.	2

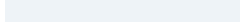


PRJ212-PH1-INS-GAD-0001-07

SR NO.	TAGS	DESCRIPTION	MANUFACTURER	PART No.	QTY.
1	–	ENCLOSURE (1200W X 800D X 2000H) WITH FRONT & REAR DOOR	RITTAL	TS. 8208.521	01 No.
2	M1, M2	FAN	RITTAL	SK 3239.100	02 Nos.
3	–	FILTER	RITTAL	SK 3239.200	02 Nos.
4	DS1, DS2	DOOR SWITCH	RITTAL	SZ 4127.010	02 Nos.
5	H1, H2	PANEL LIGHT	RITTAL	SZ 4138.180	02 Nos.
6	–	SIDE PANEL	RITTAL	TS 8108.235	1 SET
7	–	FRONT & REAR PANEL (PLINTH)	RITTAL	TS 8601.200	1 SET
8	–	PANEL PLINTH	RITTAL	TS 8601.080	1 SET
9	–	HANDLE WITH SEMI CYLINDER	RITTAL	DK 7320.721 + SZ 2467.000	02 Nos.
10	RU–1	CMC III READER UNITS	RITTAL	DK 7030.230	01 No.
11	PU–1	CMC III PROCESSING UNITS	RITTAL	DK 7030.000	01 No.
12	BA–1 & BA–2	CMC III CAN BUS ACCESS	RITTAL	DK 7030.200	02 Nos.
13	–	CMC III MOUNTING UNIT	RITTAL	DK 7030.071	01 No.
		RACK–A			
14	RACK–A	10 SLOT CHASSIS	MODICON	140 XBP 010 00	01 No.
15	G1	24V DC, RACK POWER SUPPLY UNIT	MODICON	140 CPS 214 00	01 No.
16	CPU1	PROCESSOR UN IT	MODICON	140 CPU 671 60	01 No.
17	RICH1	RIO HEAD END ADAPTER	MODICON	140 CRP 932 00	01 No.
18	NOE1 & NOE2	ETHERNET MODULE	MODICON	140 NOE 771 01	02 Nos.
19	NOM1	MODBUS PLUS MODULE	MODICON	140 NOM 212 00	01 No.
20	PM1	PROFIBUS MODULE	PROSOFT	PTQ–PDPMV1	01 No.
21	EMP1 & EMP2	DUMMY MODULE WITH COVER – FOR DISCRETE I/O MODULE	MODICON	140 XCP 510 00	02 Nos.
		RACK–B			
22	RACK–B	10 SLOT CHASSIS	MODICON	140 XBP 010 00	01 No.
23	G2	24V DC, RACK POWER SUPPLY UNIT	MODICON	140 CPS 214 00	01 No.
24	CPU2	PROCESSOR UN IT	MODICON	140 CPU 671 60	01 No.
25	RICH2	RIO HEAD END ADAPTER	MODICON	140 CRP 932 00	01 No.
26	NOE3 & NOE4	ETHERNET MODULE	MODICON	140 NOE 771 01	02 Nos.
27	NOM2	MODBUS PLUS MODULE	MODICON	140 NOM 212 00	01 No.
28	PM2	PROFIBUS MODULE	PROSOFT	PTQ–PDPMV1	01 No.
29	EMP1 & EMP2	DUMMY MODULE WITH COVER – FOR DISCRETE I/O MODULE	MODICON	140 XCP 510 00	02 Nos.
		RACK–1			
30	RACK–1	16 SLOT CHASSIS	MODICON	140 XBP 016 00	01 No.
31	G3	24V DC, RACK POWER SUPPLY UNIT	MODICON	140 CPS 214 00	01 No.
32	RIOD1	RIO DROP ADAPTER	MODICON	140 CRA 932 00	01 No.
33	DI1 – DI5	DIGITAL INPUT MODULE 32 CHANNEL	MODICON	140 DDI 353 00	05 Nos.
34	DO1 – DO2	DIGITAL OUTPUT MODULE 16 CHANNEL	MODICON	140 DDO 843 00	02 Nos.

LEGEND:

-  CONSTRUCTION SCOPE
-  REVISION CLOUD

2	06.05.18	ISSUED FOR CONSTRUCTION	SJM	JLK	NH	AA	
1	03.04.18	ISSUED FOR APPROVAL	SJM	JLK	NH	AA	
0	12.02.18	ISSUED FOR REVIEW	SAA	JLK	NH	AA	
ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD	

CLIENT	 هيئة كهرباء ومياه دبي Dubai Electricity & Water Authority	 P.O. BOX: 564, DUBAI, UAE. TEL: 00971-4-324 4444. FAX: 00971-4-324 4922	DEWA PRJ REF : RFX-2131600072 DEWA PO REF : PO: 3761700080		VENDOR  Silvertech P.O. BOX: 17910, JEBEL ALI, DUBAI, U.A.E T: +971 (4) 8995000. F: +971 (4) 8995001 www.silvertech-me.com	SCALE: N.T.S.
			DEWA DWG. NO. RFX72-PLC-GAD1			SIZE: A3
PROJECT: SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX - PHASE-1 PLC PANEL GA DRAWING - BOM			STME DWG. NO. PRJ212-PH1-INS-GAD-0001		SHEET 07 OF 10	REV. 2

PRJ212-PH1-INS-GAD-0001-08

SR NO.	TAGS	DESCRIPTION	MANUFACTURER	PART No.	QTY.
		RACK-1			
35	AI1 - AI5	ANALOG INPUT MODULE 8 CHANNEL	MODICON	140 ACI 030 00	05 Nos.
36	EMP1 & EMP2	DUMMY MODULE WITH COVER - FOR DISCRETE I/O MODULE	MODICON	140 XCP 510 00	02 Nos.
37	TAP1A & TAP1B	SPLITTER	MODICON	MA 0186 100C	02 Nos.
38	TAP2A & TAP2B	R I/O TAP	MODICON	MA 0185 100C	02 Nos.
		RACK-2			
39	RACK-2	16 SLOT CHASSIS	MODICON	140 XBP 016 00	01 No.
40	G4	24V DC, RACK POWER SUPPLY UNIT	MODICON	140 CPS 214 00	01 No.
41	RIOD2	RIO DROP ADAPTER	MODICON	140 CRA 932 00	01 No.
42	AI6 - AI12	ANALOG INPUT MODULE 8 CHANNEL	MODICON	140 ACI 030 00	07 Nos.
43	DO3	DIGITAL OUTPUT MODULE 16 CHANNEL	MODICON	140 DDO 843 00	01 No.
44	EMP1 - EMP6	DUMMY MODULE WITH COVER - FOR DISCRETE I/O MODULE	MODICON	140 XCP 510 00	06 Nos.
45	TAP2A & TAP2B	R I/O TAP	MODICON	MA 0185 100C	02 Nos.
		RAIL-A			
46	X31	FUSE TERMINAL (WSI 6)	WEIDMULLER	1011000000	20 Nos.
47	X32	FEED THROUGH TERMINAL (WDU 2.5)	WEIDMULLER	1020000000	20 Nos.
48	X33	FUSE TERMINAL (WSI 6)	WEIDMULLER	1011000000	30 Nos.
49	X34	FEED THROUGH TERMINAL (WDU 2.5)	WEIDMULLER	1020000000	30 Nos.
50	DB1 - DB2	DIODE BLACK	ST MICRO	STPS12045TV	02 Nos.
		RAIL-B			
51	PS1 & PS3	POWER SUPPLY 230V AC/24V DC 20A	PHOENIX	QUINT-PS/1AC/24DC/20	02 Nos.
52	F31 & F33	MCB 20A 2P	SCHNEIDER ELECTRIC	24338	02 Nos.
53	F32 & F34	MCB 10A 2P	SCHNEIDER ELECTRIC	24336	02 Nos.
54	PS2 & PS4	POWER SUPPLY 230V AC/24V DC 20A	PHOENIX	QUINT-PS/1AC/24DC/20	02 Nos.
55	K100 & K200	4 C/O RELAY 230V AC COIL + RELAY BASE	OMRON	MY4N-220/240VAC + PYF14-ESN	02 Nos.
56	F100 & F200	MCB 10A 2P	SCHNEIDER ELECTRIC	24336	02 Nos.
		RAIL-C			
57	X0	MCB 20A 2P	ABB	2CSR272140R1204	02 Nos.
58	X0	EARTH TERMINAL (WPE 6)	WEIDMULLER	1010200000	01 No.
59	F0	MCB 10A 2P	SCHNEIDER ELECTRIC	24336	01 No.
60	F1 - F4	MCB 6A 1P	HAGER	MW106	04 Nos.
61	X0	FEED THROUGH TERMINAL (WDU 2.5)	WEIDMULLER	1020000000	12 Nos.
62	X10	FEED THROUGH POWER TERMINAL (WDU6)	WEIDMULLER	1020200000	02 Nos.
63	X10	EARTH TERMINAL (WPE 6)	WEIDMULLER	1010200000	01 No.

LEGEND:

2	06.05.18	ISSUED FOR CONSTRUCTION	SJM	JLK	NH	AA	
1	03.04.18	ISSUED FOR APPROVAL	SJM	JLK	NH	AA	
0	12.02.18	ISSUED FOR REVIEW	SAA	JLK	NH	AA	
ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD	

CLIENT



DEWA PRJ REF : RFX-2131600072
DEWA PO REF : PO: 3761700080
DEWA DWG. NO.
RFX72-PLC-GAD1

PROJECT:

SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA
SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY
IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX - PHASE-1 PLC PANEL GA DRAWING - BOM

VENDOR



STME DWG. NO.
PRJ212-PH1-INS-GAD-0001

SHEET
08 OF 10

SCALE:

N.T.S.

SIZE:

A3

REV.

2

PRJ212-PH1-INS-GAD-0001-09

SR NO.	TAGS	DESCRIPTION	MANUFACTURER	PART No.	QTY.
		RAIL-C			
64	F10	MCB 10A 2P	SCHNEIDER ELECTRIC	24336	01 No.
65	F11 – F14	MCB 6A 1P	HAGER	MW106	04 Nos.
66	X11	FEED THROUGH TERMINAL (WDU 2.5)	WEIDMULLER	1020000000	04 Nos.
67	X20	FEED THROUGH POWER TERMINAL (WDU6)	WEIDMULLER	1020200000	02 Nos.
68	X20	EARTH TERMINAL (WPE 6)	WEIDMULLER	1010200000	01 No.
69	F20	MCB 10A 2P	SCHNEIDER ELECTRIC	24336	01 No.
70	F21 – F24	MCB 6A 1P	HAGER	MW106	04 Nos.
71	X21	FEED THROUGH TERMINAL (WDU 2.5)	WEIDMULLER	1020000000	04 Nos.
72	X12 & X22	FUSE TERMINAL (WSI 6)	WEIDMULLER	1011000000	EACH 06
73		FEED THROUGH TERMINAL (WDU 2.5)	WEIDMULLER	1020000000	EACH 12
		RAIL-D			
74	ES1 & ES2	ETHERNET SWITCH	KORENIEX	JETNET 4510	02 Nos.
75	HAI	ANALOG HART MODULE	PROSOFT	5208 MNET-HART	01 No.
76	MCM1 & MCM2	MODBUS MODULE	PROSOFT	5302-MBP-MCM4	02 Nos.
77	K1 – K32	PLUGGABLE RELAY, CR-P024DC2, 2 C/O, 250V, 8A, 24VDC	ABB	1SVR405601R1000	32 Nos.
78		SOCKET, CR-PLS, LOGICAL SOCKET WITH SAFETY ISOLATION	ABB	1SVR405650R0000	32 Nos.
79		SOCKET ACCESSORIES, CR-PH, PLASTIC HOLDER	ABB	1SVR405659R0000	32 Nos.
80		DIODE AND LED, CR-P/M 42V, 6-24VDC, GREEN	ABB	1SVR405652R1000	32 Nos.
		RAIL-E			
81	XDI1 – XDI2	FUSE TERMINAL (WSI 6)	WEIDMULLER	1011000000	EACH 32
82		DISCONNECTOR TERMINAL (WTR 2.5)	WEIDMULLER	1855610000	EACH 32
83	XDO1	FUSE TERMINAL (WSI 6)	WEIDMULLER	1011000000	32 Nos.
84		DISCONNECTOR TERMINAL (WTR 2.5)	WEIDMULLER	1855610000	32 Nos.
		RAIL-F			
85	XDI3 – XDI4	FUSE TERMINAL (WSI 6)	WEIDMULLER	1011000000	EACH 32
86		DISCONNECTOR TERMINAL (WTR 2.5)	WEIDMULLER	1855610000	EACH 32
87	XDO2	FUSE TERMINAL (WSI 6)	WEIDMULLER	1011000000	32 Nos.
88		DISCONNECTOR TERMINAL (WTR 2.5)	WEIDMULLER	1855610000	32 Nos.
		RAIL-G			
89	XDI5	FUSE TERMINAL (WSI 6)	WEIDMULLER	1011000000	32 Nos.
90		DISCONNECTOR TERMINAL (WTR 2.5)	WEIDMULLER	1855610000	EACH 32
91	K33- K48	PLUGGABLE RELAY, CR-P024DC2, 2 C/O, 250V, 8A, 24VDC	ABB	1SVR405601R1000	32 Nos.
92		SOCKET, CR-PLS, LOGICAL SOCKET WITH SAFETY ISOLATION	ABB	1SVR405650R0000	32 Nos.
93		SOCKET ACCESSORIES, CR-PH, PLASTIC HOLDER	ABB	1SVR405659R0000	32 Nos.
94		DIODE AND LED, CR-P/M 42V, 6-24VDC, GREEN	ABB	1SVR405652R1000	32 Nos.

LEGEND:

- CONSTRUCTION SCOPE
- REVISION CLOUD

2	06.05.18	ISSUED FOR CONSTRUCTION	SJM	JLK	NH	AA	
1	03.04.18	ISSUED FOR APPROVAL	SJM	JLK	NH	AA	
0	12.02.18	ISSUED FOR REVIEW	SAA	JLK	NH	AA	
ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD	

CLIENT	<div><div>هيئة كهرباء ومياه دبي</div><div>Dubai Electricity & Water Authority</div><div><div></div><div></div></div></div> <div>P.O. BOX: 564, DUBAI, UAE. TEL: 00971-4-324 4444. FAX: 00971-4-324 4922</div>	DEWA PRJ REF : RFX-2131600072
		DEWA PD REF : PD: 3761700080
PROJECT:	SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX - PHASE-1 PLC PANEL GA DRAWING - BOM	DEWA DWG. NO. RFX72-PLC-GAD1

VENDOR	
<div><div></div><div>Silvertech</div><div><div>P.O. BOX: 17910, JEBEL ALI, DUBAI, U.A.E</div><div>T: +971 (4) 8995000. F: +971 (4) 8995001</div><div>www.silvertech-me.com</div></div></div>	
STME DWG. NO.	SHEET
PRJ212-PH1-INS-GAD-0001	09 OF 10

SCALE:
N.T.S.
SIZE:
A3
REV.
2

SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX

GENERAL ARRANGEMENT DRAWING
PHASE-2 PLC PANEL

REFERENCE DRAWINGS/DOCUMENTS:

2	06.05.18	ISSUED FOR CONSTRUCTION	SJM	JLK	NH	AA	
1	03.04.18	ISSUED FOR APPROVAL	SJM	JLK	NH	AA	
0	12.02.18	ISSUED FOR REVIEW	SAA	JLK	NH	AA	
ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD	

CLIENT

هيئة كهرباء ومياه دبي

Dubai Electricity & Water Authority

P.O. BOX: 564, DUBAI, UAE. TEL: 00971-4-324 4444. FAX: 00971-4-324 4922

DEWA PRJ REF : RFX-2131600072


DEWA PO REF : PO: 3761700080

DEWA DWG. NO. RFX72-PLC-GAD2

PROJECT:

SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX - PHASE-2 PLC PANEL GA DRAWING - COVER SHEET

VENDOR

Silvertech

P.O. BOX: 17910, JEBEL ALI, DUBAI, U.A.E
T: +971 (4) 8995000, F: +971 (4) 8995001
www.silvertech-me.com

STME DWG. NO.

PRJ212-PH2-INS-GAD-0001

SHEET

01 OF 10

SCALE:

N.T.S.

SIZE:

A3

REV.

2

PRJ212-PH2-INS-GAD-0001-02

SHEET NO.	DESCRIPTION	FILE NAME	DATE	REVISIONS				PURPOSE OF ISSUE
				0	1	2	3	
1	PHASE-2 PLC PANEL GENERAL ARRANGEMENT DRAWING - COVER SHEET	PRJ212-PH2-INS-GAD-0001-01	06.05.18	X	X	X		ISSUED FOR CONSTRUCTION
2	PHASE-2 PLC PANEL GENERAL ARRANGEMENT DRAWING - INDEX SHEET	PRJ212-PH2-INS-GAD-0001-02	06.05.18	X	X	X		ISSUED FOR CONSTRUCTION
3	PHASE-2 PLC PANEL GENERAL ARRANGEMENT DRAWING	PRJ212-PH2-INS-GAD-0001-03	06.05.18	X	X	X		ISSUED FOR CONSTRUCTION
4	PHASE-2 PLC PANEL GENERAL ARRANGEMENT DRAWING	PRJ212-PH2-INS-GAD-0001-04	06.05.18	X	X	X		ISSUED FOR CONSTRUCTION
5	PHASE-2 PLC PANEL GENERAL ARRANGEMENT DRAWING	PRJ212-PH2-INS-GAD-0001-05	06.05.18	X	X	X		ISSUED FOR CONSTRUCTION
6	PHASE-2 PLC PANEL GENERAL ARRANGEMENT DRAWING - RACK DETAILS	PRJ212-PH2-INS-GAD-0001-06	06.05.18	X	X	X		ISSUED FOR CONSTRUCTION
7	PHASE-2 PLC PANEL GENERAL ARRANGEMENT DRAWING - BILL OF MATERIAL	PRJ212-PH2-INS-GAD-0001-07	06.05.18	X	X	X		ISSUED FOR CONSTRUCTION
8	PHASE-2 PLC PANEL GENERAL ARRANGEMENT DRAWING - BILL OF MATERIAL	PRJ212-PH2-INS-GAD-0001-08	06.05.18	X	X	X		ISSUED FOR CONSTRUCTION
9	PHASE-2 PLC PANEL GENERAL ARRANGEMENT DRAWING - BILL OF MATERIAL	PRJ212-PH2-INS-GAD-0001-09	06.05.18	X	X	X		ISSUED FOR CONSTRUCTION
10	PHASE-2 PLC PANEL GENERAL ARRANGEMENT DRAWING - BILL OF MATERIAL	PRJ212-PH2-INS-GAD-0001-10	06.05.18	X	X	X		ISSUED FOR CONSTRUCTION
11								
12								
13								
14								
15								
16								
17								
18								
19								
20								
21								
22								
23								
24								
25								
26								
27								
28								
29								
30								
31								
32								
33								
34								
35								
36								
37								
38								

REFERENCE DRAWINGS/DOCUMENTS:

2	06.05.18	ISSUED FOR CONSTRUCTION	SJM	JLK	NH	AA	
1	03.04.18	ISSUED FOR APPROVAL	SJM	JLK	NH	AA	
0	12.02.18	ISSUED FOR REVIEW	SAA	JLK	NH	AA	
ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD	

CLIENT

هيئة كهرباء ومياه دبي

Dubai Electricity & Water Authority



DEWA PRJ REF : RFX-2131600072


DEWA PO REF : PO: 3761700080

DEWA DWG. NO. RFX72-PLC-GAD2

PROJECT:

SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX - PHASE-2 PLC PANEL GA DRAWING-INDEX SHEET

VENDOR



Silvertech

سولڤرٲيٲ

P.O. BOX: 17910, JEBEL ALI, DUBAI, U.A.E

T: +971 (4) 8995000, F: +971 (4) 8995001

www.silvertech-me.com

STME DWG. NO.

PRJ212-PH2-INS-GAD-0001

SHEET

02 OF 10

SCALE:

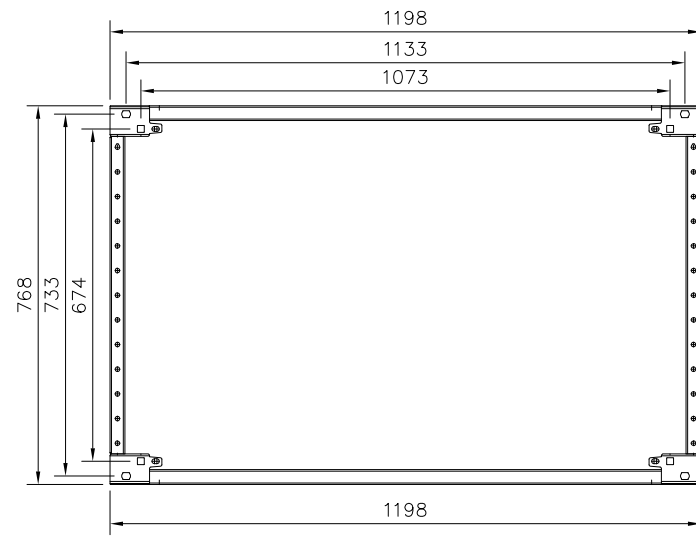
N.T.S.

SIZE:

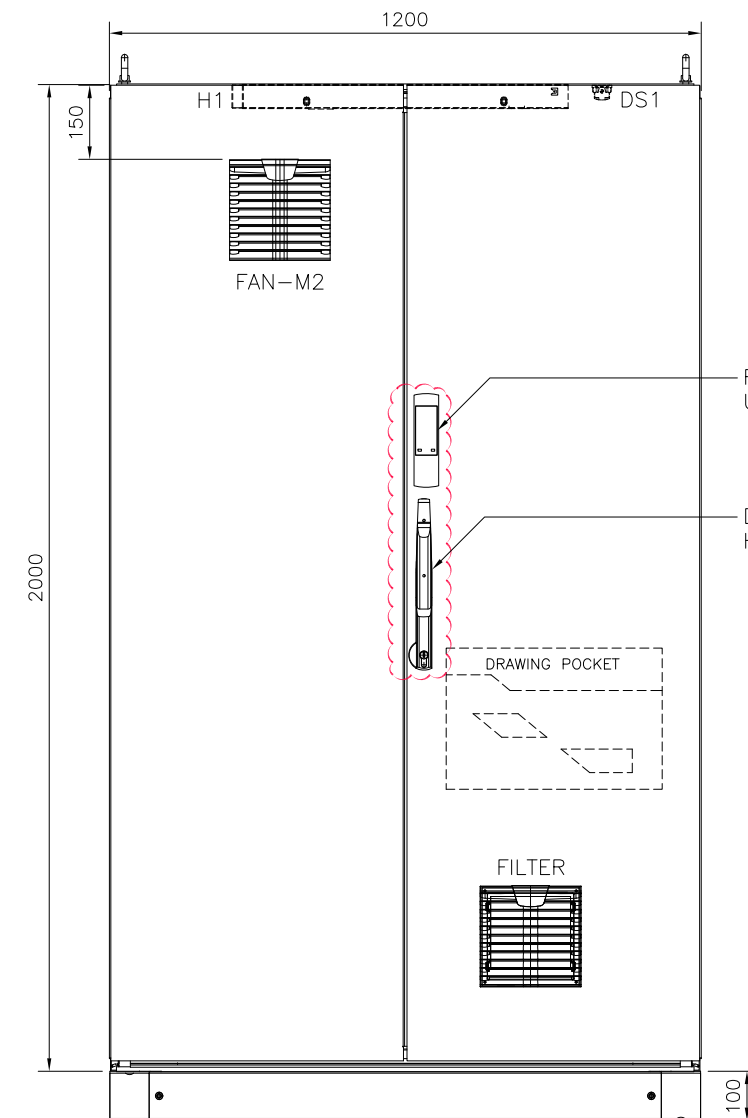
A3

REV.

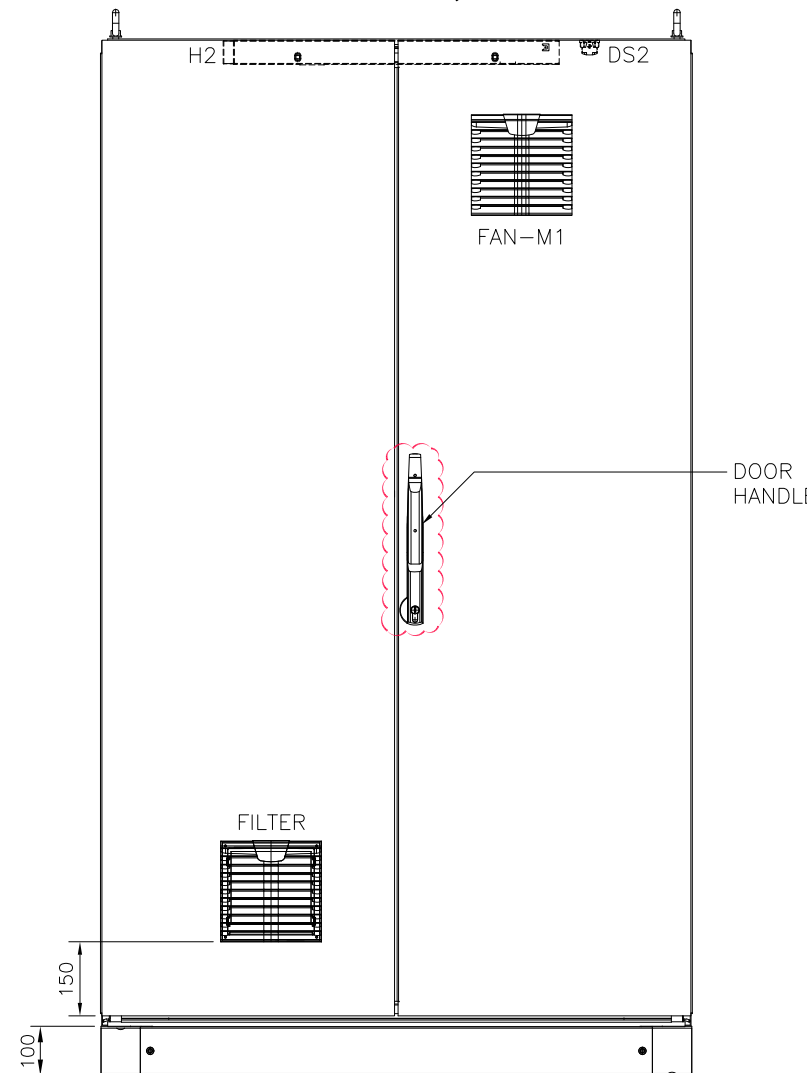
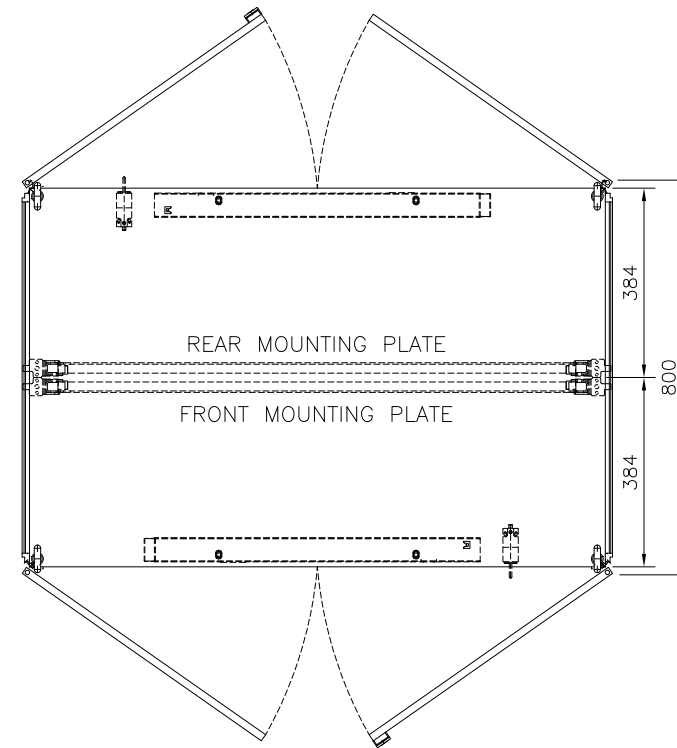
2



PLINTH TOP VIEW



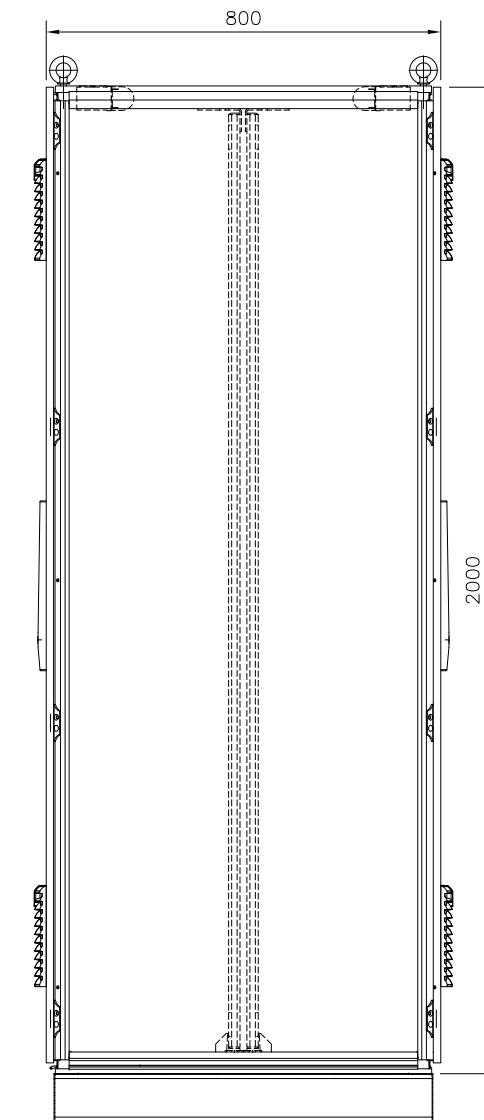
FRONT VIEW WITH DOOR



REAR VIEW WITH DOOR

NOTES:

1. RITTAL ENCLOSURE: TS 8208.521 (WITH FRONT AND REAR DOOR)
2. ENCLOSURE FRAME: DIPCOAT PRIMED IN RAL 7035 1.5MM THICK SHEET STEEL.
3. DOORS: DIPCOAT PRIMED AND POWDER AND POWDER COATED IN TEXTURED RAL 7035 2MM THICK SHEET STEEL.
4. ROOF: DIPCOAT PRIMED AND POWDER COATED IN TEXTURED RAL 7035 1.5MM THICK SHEET STEEL.
5. MOUNTING PLATE: ZINC PLATED 3MM THICK SHEET STEEL.
6. PLINTH: RAL 7022 SHEET STEEL.
7. PROTECTION CATEGORY: IP54 TO EN 60529/10.91
8. COMPLIES WITH: NEMA 12
9. CABLE ENTRY & EXIT: BOTTOM.



SIDE VIEW

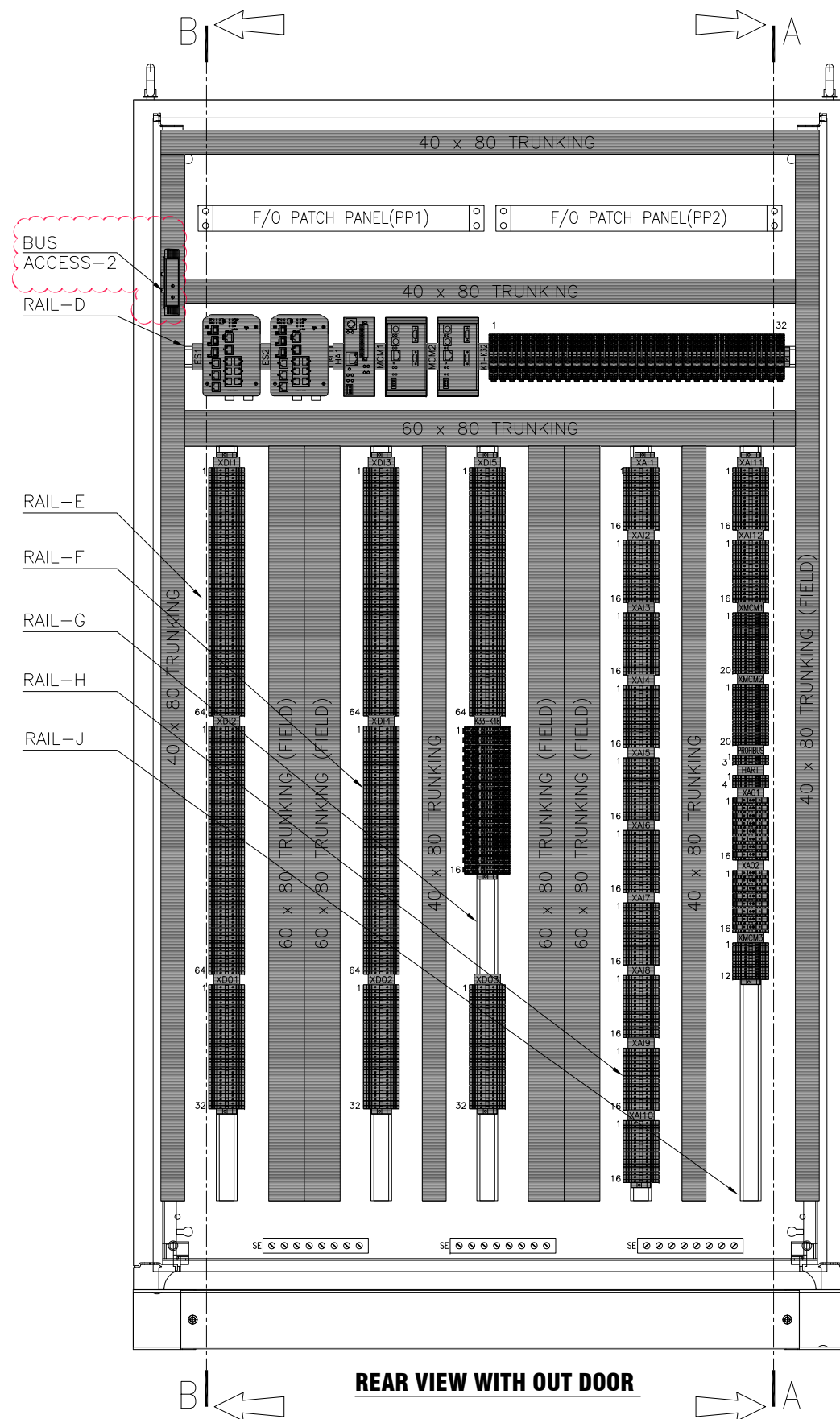
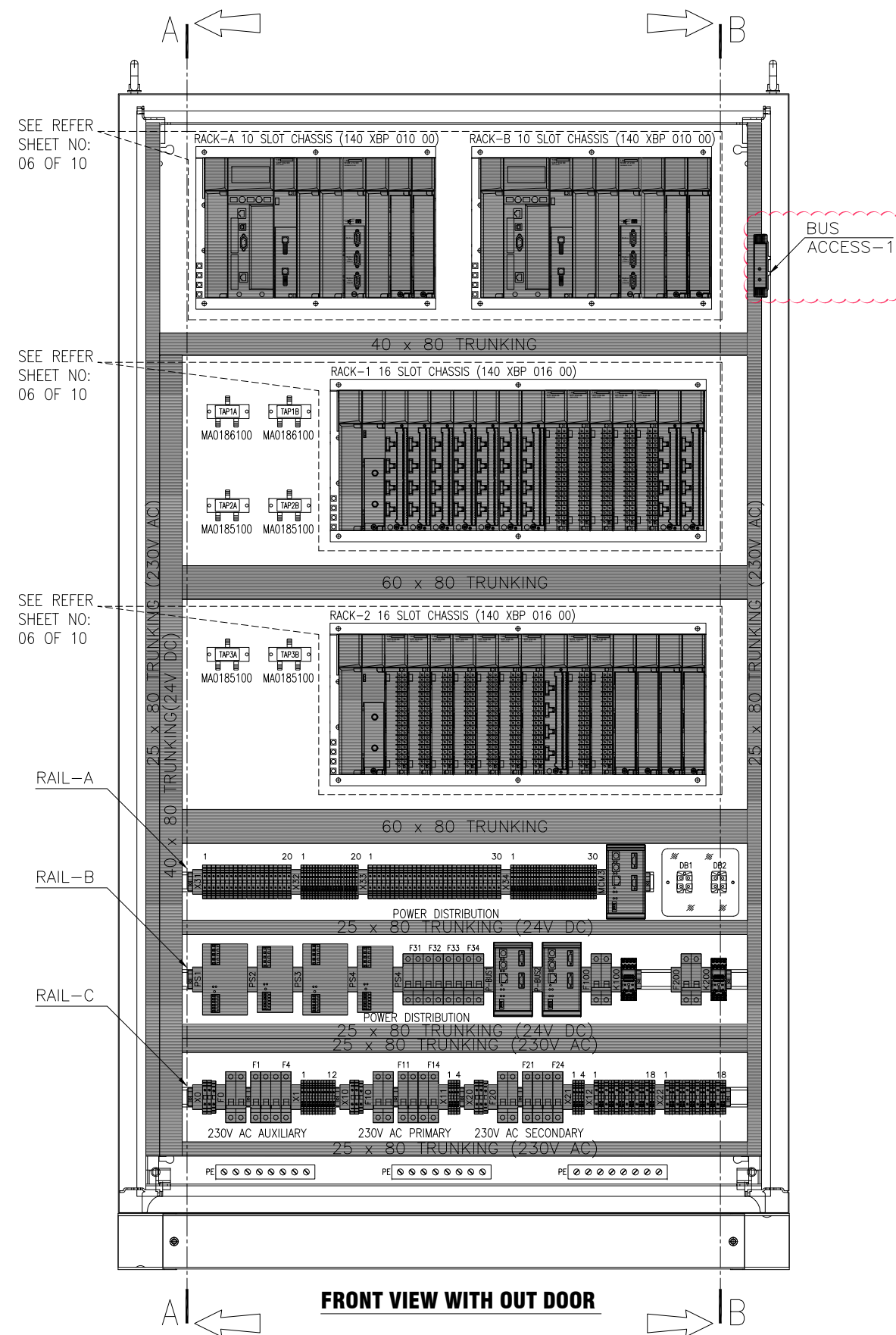
LEGEND:

- CONSTRUCTION SCOPE
- REVISION CLOUD

ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD
2	06.05.18	ISSUED FOR CONSTRUCTION	SJM	JLK	NH	AA
1	03.04.18	ISSUED FOR APPROVAL	SJM	JLK	NH	AA
0	12.02.18	ISSUED FOR REVIEW	SAA	JLK	NH	AA

CLIENT هيئة كهرباء ومياه دبي Dubai Electricity & Water Authority P.O. BOX: 564, DUBAI, UAE. TEL: 00971-4-324 4444. FAX: 00971-4-324 4922	DEWA PRJ REF : RFX-2131600072 DEWA PO REF : PO: 3761700080 DEWA DWG. NO. RFX72-PLC-GAD2	VENDOR P.O. BOX: 17910, JEBEL ALI, DUBAI, U.A.E T: +971 (4) 8995000, F: +971 (4) 8995001 www.silvertech-me.com	SCALE: 1 : 15 SIZE: A3
PROJECT: SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX - PHASE-2 PLC PANEL GA DRAWING	STME DWG. NO. PRJ212-PH2-INS-GAD-0001	SHEET 03 OF 10	REV. 2

PRJ212-PH2-INS-GAD-0001-03



LEGEND:

- CONSTRUCTION SCOPE
- REVISION CLOUD

ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD
2	06.05.18	ISSUED FOR CONSTRUCTION	SJM	JLK	NH	AA
1	03.04.18	ISSUED FOR APPROVAL	SJM	JLK	NH	AA
0	12.02.18	ISSUED FOR REVIEW	SAA	JLK	NH	AA

CLIENT

هيئة كهرباء ومياه دبي
Dubai Electricity & Water Authority

DEWA PRJ REF : RFX-2131600072
DEWA PO REF : PO: 3761700080
DEWA DWG. NO.
RFX72-PLC-GAD2

VENDOR

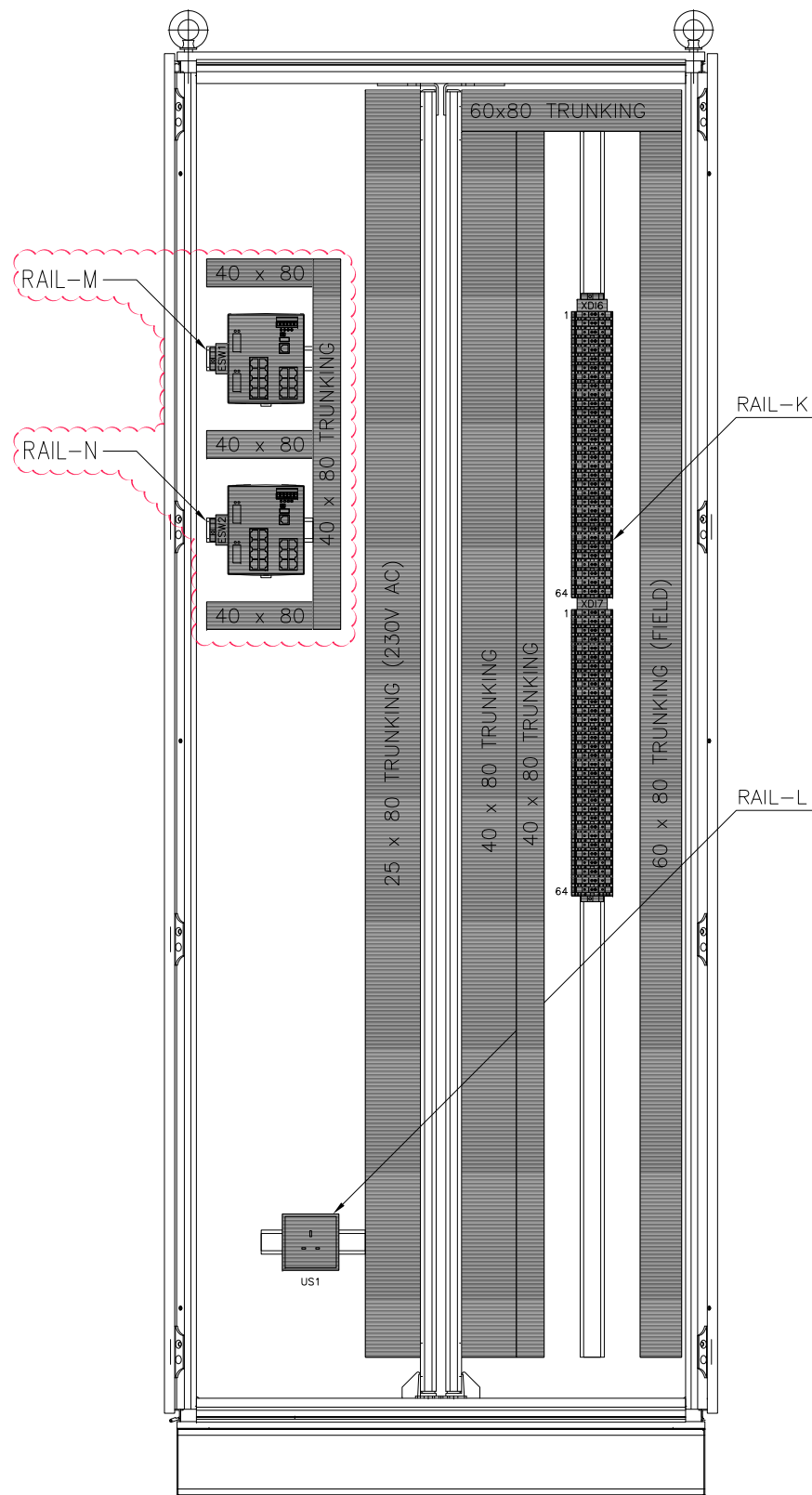
Silvertech
P.O. BOX: 17910, JEBEL ALI, DUBAI, U.A.E.
T: +971 (4) 8995000, F: +971 (4) 8995001
www.silvertch-me.com

STME DWG. NO.
PRJ212-PH2-INS-GAD-0001

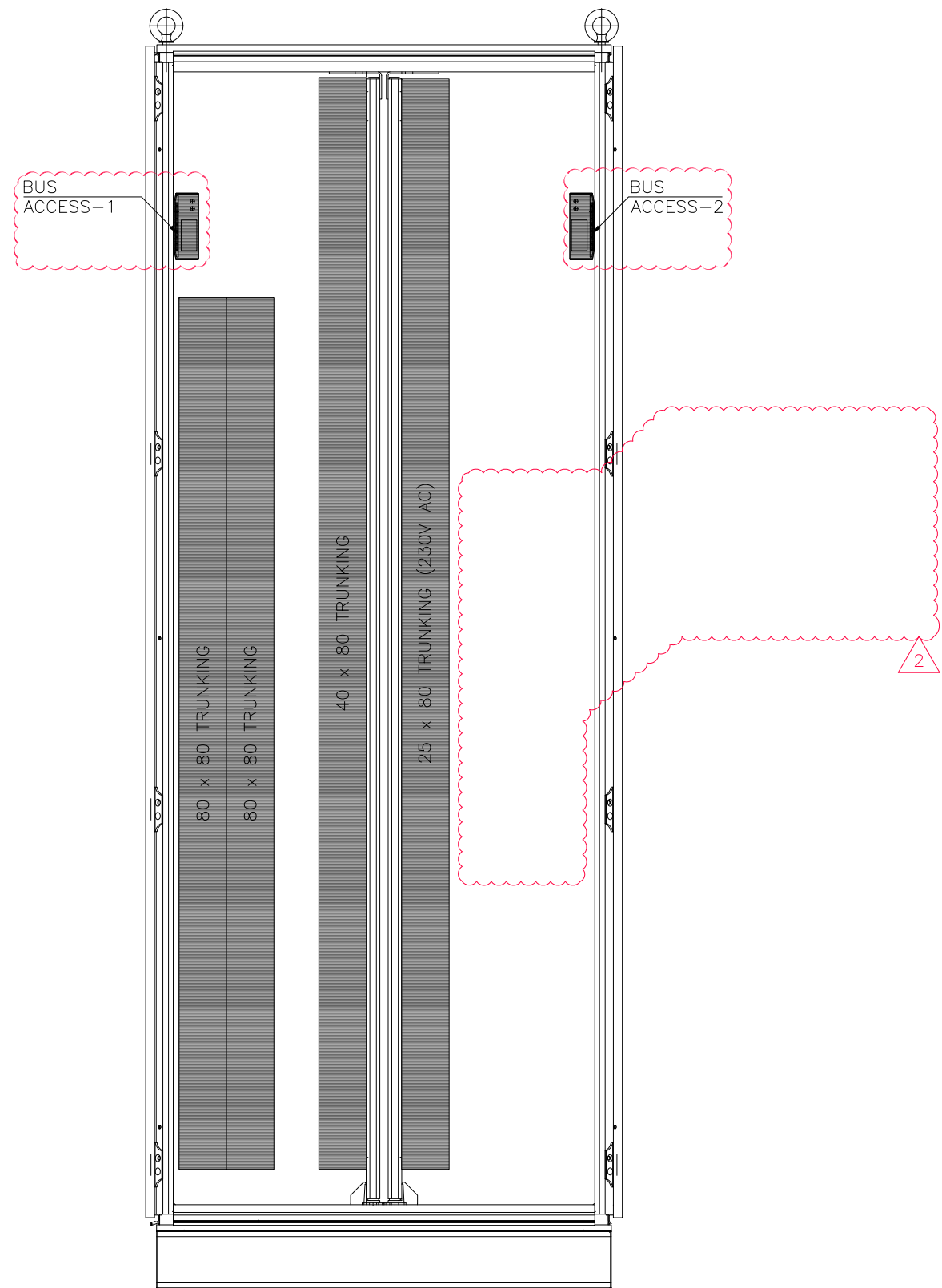
SHEET
04 OF 10

SCALE:
1 : 10
SIZE:
A3
REV.
2

PRJ212-PH2-INS-GAD-0001-05



"A-A" VIEW



"B-B" VIEW

LEGEND:

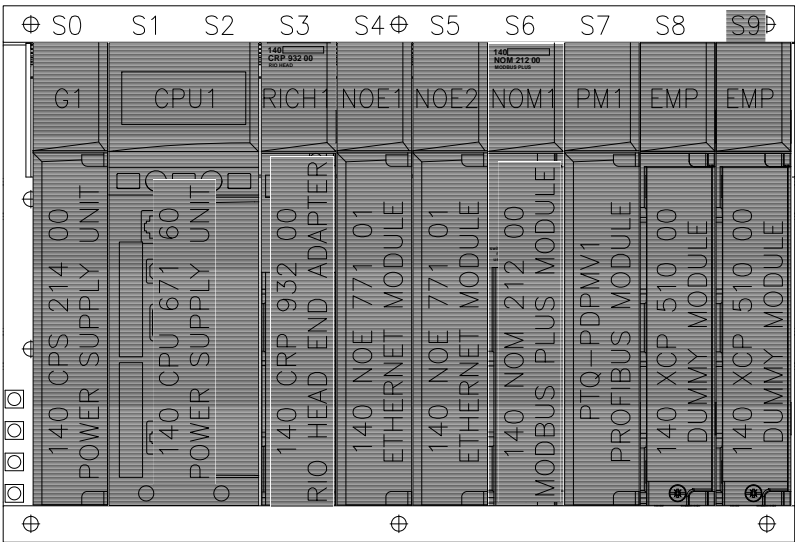
- CONSTRUCTION SCOPE
- REVISION CLOUD

ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD
2	06.05.18	ISSUED FOR CONSTRUCTION	SJM	JLK	NH	AA
1	03.04.18	ISSUED FOR APPROVAL	SJM	JLK	NH	AA
0	12.02.18	ISSUED FOR REVIEW	SAA	JLK	NH	AA

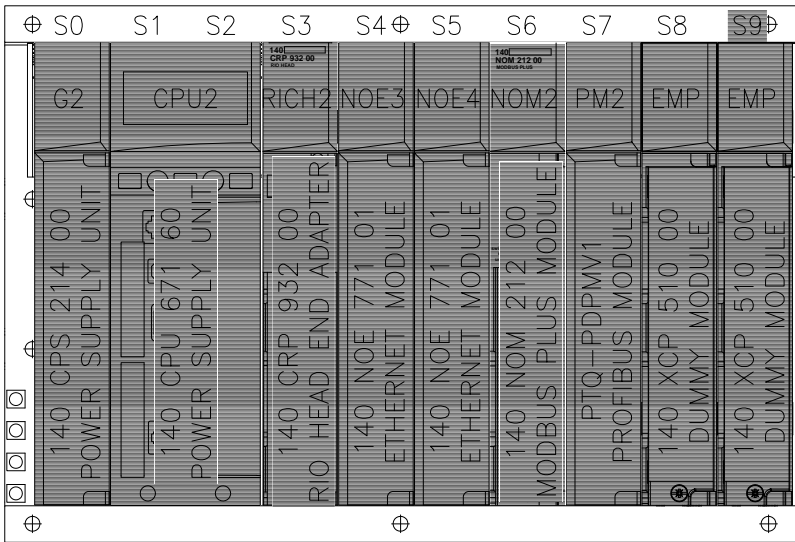
CLIENT	DEWA PRJ REF : RFX-2131600072 DEWA PO REF : PO: 3761700080
PROJECT:	DEWA DWG. NO. RFX72-PLC-GAD2
SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX - PHASE-2 PLC PANEL GA DRAWING	

VENDOR	SCALE:
Silvertech	1 : 10
P.O. BOX: 17910, JEBEL ALI, DUBAI, U.A.E. T: +971 (4) 8995000, F: +971 (4) 8995001 www.silvertch-me.com	SIZE:
STME DWG. NO. PRJ212-PH2-INS-GAD-0001	A3
SHEET 05 OF 10	REV.
	2

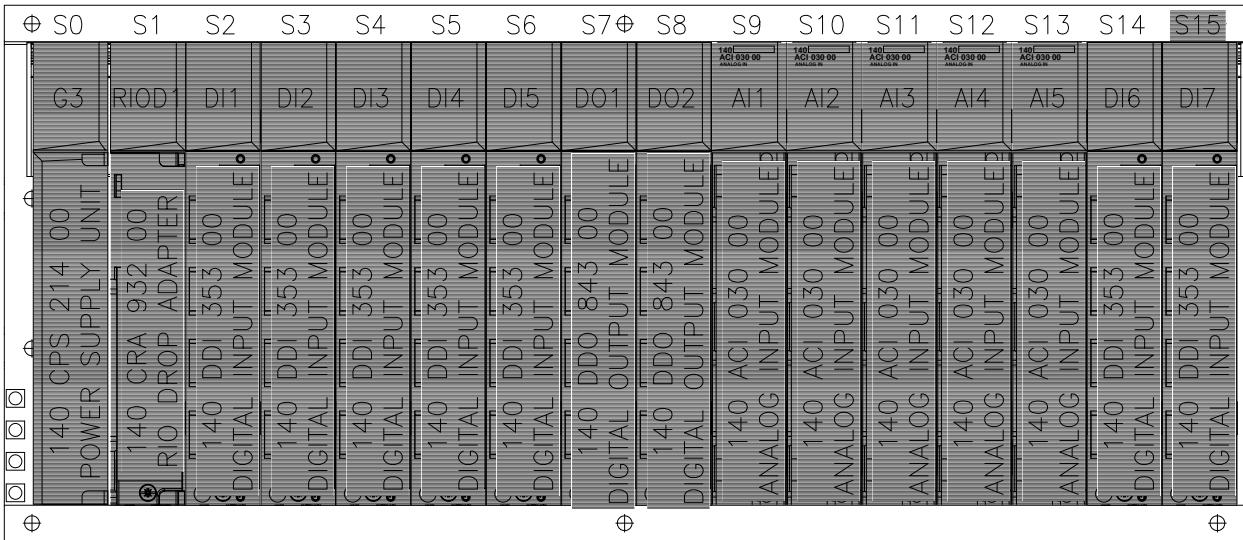
PRJ212-PH2-INS-GAD-0001-06



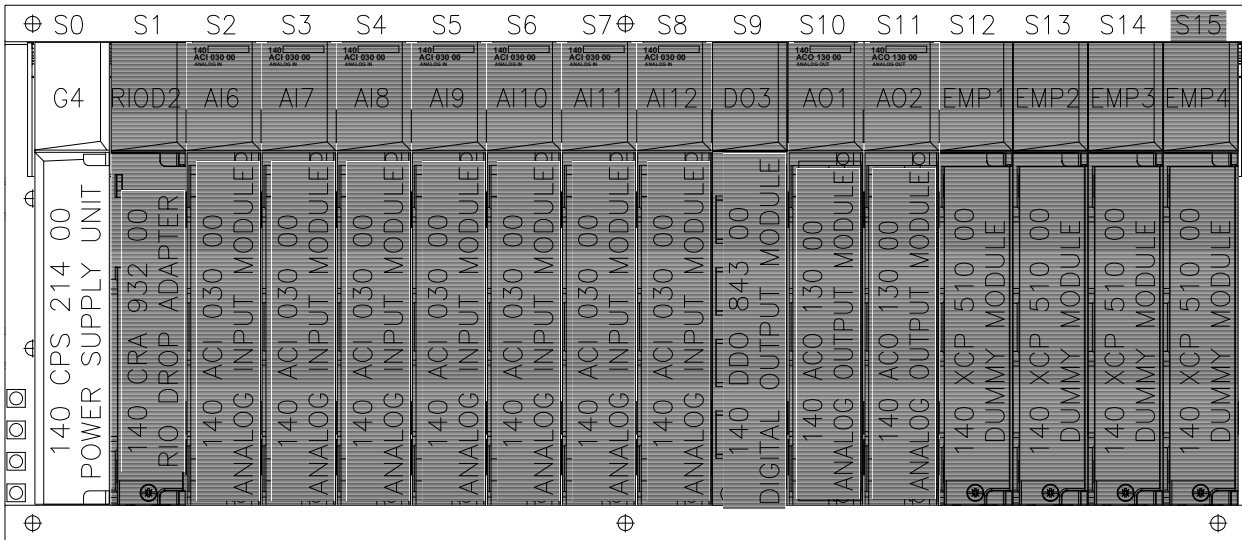
RACK-A 10 SLOT CHASSIS (140 XBP 010 00)



RACK-B 10 SLOT CHASSIS (140 XBP 010 00)



RACK-1 16 SLOT CHASSIS (140 XBP 016 00)




RACK-2 16 SLOT CHASSIS (140 XBP 016 00)

RACK DETAILS

REFERENCE DRAWINGS/DOCUMENTS:

2	06.05.18	ISSUED FOR CONSTRUCTION	SJM	JLK	NH	AA	
1	03.04.18	ISSUED FOR APPROVAL	SJM	JLK	NH	AA	
0	12.02.18	ISSUED FOR REVIEW	SAA	JLK	NH	AA	
ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD	

CLIENT	 P.O. BOX: 564, DUBAI, UAE. TEL: 00971-4-324 4444. FAX: 00971-4-324 4922	DEWA PRJ REF : RFX-2131600072 DEWA PO REF : PO: 3761700080 DEWA DWG. NO. RFX72-PLC-GAD2
PROJECT:	SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX - PHASE-2 PLC PANEL GA DRAWING-RACK DETAILS	



VENDOR	
 <div>Silvertech <small>Building the Future of the Middle East</small></div> <p>P.O. BOX: 17910, JEBEL ALI, DUBAI, U.A.E T: +971 (4) 8995000, F: +971 (4) 8995001 www.silvertech-me.com</p>	
STME DWG. NO.	SHEET
PRJ212-PH2-INS-GAD-0001	06 OF 10

SCALE:	N.T.S.
SIZE:	A3
REV.	2

PRJ212-PH2-INS-GAD-0001-07

SR NO.	TAGS	DESCRIPTION	MANUFACTURER	PART No.	QTY.
1	–	ENCLOSURE (1200W X 800D X 2000H) WITH FRONT & REAR DOOR	RITTAL	TS. 8208.521	01 No.
2	M1, M2	FAN	RITTAL	SK 3239.100	02 Nos.
3	–	FILTER	RITTAL	SK 3239.200	02 Nos.
4	DS1, DS2	DOOR SWITCH	RITTAL	SZ 4127.010	02 Nos.
5	H1, H2	PANEL LIGHT	RITTAL	SZ 4138.180	02 Nos.
6	–	SIDE PANEL	RITTAL	TS 8108.235	1 SET
7	–	FRONT & REAR PANEL (PLINTH)	RITTAL	TS 8601.200	1 SET
8	–	PANEL PLINTH	RITTAL	TS 8601.080	1 SET
9	–	HANDLE WITH SEMI CYLINDER	RITTAL	DK 7320.721 + SZ 2467.000	02 Nos.
10	RU–1	CMC III READER UNITS	RITTAL	DK 7030.230	01 No.
11					
12	BA–1 & BA–2	CMC III CAN BUS ACCESS	RITTAL	DK 7030.200	02 Nos.
13					
		RACK–A			
14	RACK–A	10 SLOT CHASSIS	MODICON	140 XBP 010 00	01 No.
15	G1	24V DC, RACK POWER SUPPLY UNIT	MODICON	140 CPS 214 00	01 No.
16	CPU1	PROCESSOR UN IT	MODICON	140 CPU 671 60	01 No.
17	RICH1	RIO HEAD END ADAPTER	MODICON	140 CRP 932 00	01 No.
18	NOE1 & NOE2	ETHERNET MODULE	MODICON	140 NOE 771 01	02 Nos.
19	NOM1	MODBUS PLUS MODULE	MODICON	140 NOM 212 00	01 No.
20	PM1	PROFIBUS MODULE	PROSOFT	PTQ–PDPMV1	01 No.
21	EMP1 & EMP2	DUMMY MODULE WITH COVER – FOR DISCRETE I/O MODULE	MODICON	140 XCP 510 00	02 Nos.
		RACK–B			
22	RACK–B	10 SLOT CHASSIS	MODICON	140 XBP 010 00	01 No.
23	G2	24V DC, RACK POWER SUPPLY UNIT	MODICON	140 CPS 214 00	01 No.
24	CPU2	PROCESSOR UN IT	MODICON	140 CPU 671 60	01 No.
25	RICH2	RIO HEAD END ADAPTER	MODICON	140 CRP 932 00	01 No.
26	NOE3 & NOE4	ETHERNET MODULE	MODICON	140 NOE 771 01	02 Nos.
27	NOM2	MODBUS PLUS MODULE	MODICON	140 NOM 212 00	01 No.
28	PM2	PROFIBUS MODULE	PROSOFT	PTQ–PDPMV1	01 No.
29	EMP1 & EMP2	DUMMY MODULE WITH COVER – FOR DISCRETE I/O MODULE	MODICON	140 XCP 510 00	02 Nos.
		RACK–1			
30	RACK–1	16 SLOT CHASSIS	MODICON	140 XBP 016 00	01 No.
31	G3	24V DC, RACK POWER SUPPLY UNIT	MODICON	140 CPS 214 00	01 No.
32	RIOD1	RIO DROP ADAPTER	MODICON	140 CRA 932 00	01 No.
33	DI1 – DI7	DIGITAL INPUT MODULE 32 CHANNEL	MODICON	140 DDI 353 00	07 Nos.
34	DO1 – DO2	DIGITAL OUTPUT MODULE 16 CHANNEL	MODICON	140 DDO 843 00	02 Nos.
35	AI1 – AI5	ANALOG INPUT MODULE 8 CHANNEL	MODICON	140 ACI 030 00	05 Nos.

LEGEND:

-  CONSTRUCTION SCOPE
-  REVISION CLOUD

2	06.05.18	ISSUED FOR CONSTRUCTION	SJM	JLK	NH	AA	
1	03.04.18	ISSUED FOR APPROVAL	SJM	JLK	NH	AA	
0	12.02.18	ISSUED FOR REVIEW	SAA	JLK	NH	AA	
ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD	

CLIENT



هيئة كهرباء ومياه دبي
Dubai Electricity & Water Authority



DEWA PRJ REF : RFX-2131600072
DEWA PO REF : PO: 3761700080
DEWA DWG. NO.
RFX72-PLC-GAD2

PROJECT:
SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA
SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY
IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX - PHASE-2 PLC PANEL GA DRAWING - BOM

VENDOR



Silvertech

P.O. BOX: 17910, JEBEL ALI, DUBAI, U.A.E
T: +971 (4) 8995000, F: +971 (4) 8995001
www.silvertech-me.com

STME DWG. NO.
PRJ212-PH2-INS-GAD-0001

SHEET
07 OF 10





SCALE:
N.T.S.
SIZE:
A3
REV.
2

PRJ212-PH2-INS-GAD-0001-08

SR NO.	TAGS	DESCRIPTION	MANUFACTURER	PART No.	QTY.
36	TAP1A & TAP1B	SPLITTER	MODICON	MA 0186 100C	02 Nos.
37	TAP2A & TAP2B	R I/O TAP	MODICON	MA 0185 100C	02 Nos.
		RACK-2			
38	RACK-2	16 SLOT CHASSIS	MODICON	140 XBP 016 00	01 No.
39	G4	24V DC, RACK POWER SUPPLY UNIT	MODICON	140 CPS 214 00	01 No.
40	RIOD2	RIO DROP ADAPTER	MODICON	140 CRA 932 00	01 No.
41	AI6 – AI12	ANALOG INPUT MODULE 8 CHANNEL	MODICON	140 ACI 030 00	07 Nos.
42	DO3	DIGITAL OUTPUT MODULE 16 CHANNEL	MODICON	140 DDO 843 00	01 No.
43	AO1 – AO2	ANALOG OUTPUT MODULE 8 CHANNEL	MODICON	140 ACO 130 00	02 Nos.
44	EMP1 – EMP4	DUMMY MODULE WITH COVER – FOR DISCRETE I/O MODULE	MODICON	140 XCP 510 00	04 Nos.
45	TAP2A & TAP2B	R I/O TAP	MODICON	MA 0185 100C	02 Nos.
		RAIL-A			
46	X31	FUSE TERMINAL (WSI 6)	WEIDMULLER	1011000000	20 Nos.
47	X32	FEED THROUGH TERMINAL (WDU 2.5)	WEIDMULLER	1020000000	20 Nos.
48	X33	FUSE TERMINAL (WSI 6)	WEIDMULLER	1011000000	30 Nos.
49	X34	FEED THROUGH TERMINAL (WDU 2.5)	WEIDMULLER	1020000000	30 Nos.
50	MCM3	MODBUS MODULE (MODBUS TO MODBUS)	PROSOFT	5302-MBP-MCM4	01 No.
51	DB1 – DB2	DIODE BLACK	ST MICRO	STPS12045TV	02 Nos.
		RAIL-B			
52	PS1 & PS3	POWER SUPPLY 230V AC/24V DC 20A	SCHNEIDER ELECTRIC	ABL 4RSM24200	02 Nos.
53	PS2 & PS4	POWER SUPPLY 230V AC/24V DC 10A	SCHNEIDER ELECTRIC	ABL 4RSM24100	02 Nos.
54	F31 – F34	MCB 10A 2P	SCHNEIDER ELECTRIC	24336	04 Nos.
55	P-BUS1 & P-BUS2	MODBUS MODULE (MODBUS TO MODBUS)	PROSOFT	5302-MBP-MCM4	02 Nos.
56	F100 & F200	MCB 10A 2P	SCHNEIDER ELECTRIC	24336	02 Nos.
57	K100 & K200	4 C/O RELAY 230V AC COIL + RELAY BASE	OMRON	MY4N-220/240VAC + PYF14-ESN	02 Nos.
		RAIL-C			
58	X0	MCB 20A 2P	SCHNEIDER ELECTRIC	24338	02 Nos.
59	X0	EARTH TERMINAL (WPE 6)	WEIDMULLER	1010200000	01 No.
60	F0	MCB 10A 2P	SCHNEIDER ELECTRIC	24336	01 No.
61	F1 – F4	MCB 6A 1P	HAGER	MW106	04 Nos.
62	X0	FEED THROUGH TERMINAL (WDU 2.5)	WEIDMULLER	1020000000	12 Nos.
63	X10	FEED THROUGH POWER TERMINAL (WDU6)	WEIDMULLER	1020200000	02 Nos.
64	X10	EARTH TERMINAL (WPE 6)	WEIDMULLER	1010200000	01 No.
65	F10	MCB 10A 2P	SCHNEIDER ELECTRIC	24336	01 No.
66	F11 – F14	MCB 6A 1P	HAGER	MW106	04 Nos.

LEGEND:

2	06.05.18	ISSUED FOR CONSTRUCTION	SJM	JLK	NH	AA	
1	03.04.18	ISSUED FOR APPROVAL	SJM	JLK	NH	AA	
0	12.02.18	ISSUED FOR REVIEW	SAA	JLK	NH	AA	
ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD	

CLIENT	 هيئة كهرباء ومياه دبي Dubai Electricity & Water Authority	 P.O. BOX: 564, DUBAI, UAE. TEL: 00971-4-324 4444. FAX: 00971-4-324 4922	DEWA PRJ REF : RFX-2131600072 DEWA PO REF : PO: 3761700080		VENDOR   P.O. BOX: 17910, JEBEL ALI, DUBAI, U.A.E T: +971 (4) 8995000. F: +971 (4) 8995001 www.silvertech-me.com	SCALE: N.T.S.
			DEWA DWG. NO. RFX72-PLC-GAD2			SIZE: A3
PROJECT: SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX - PHASE-2 PLC PANEL GA DRAWING - BOM			STME DWG. NO. PRJ212-PH2-INS-GAD-0001	SHEET 08 OF 10	REV. 2	

PRJ212-PH2-INS-GAD-0001-09

SR NO.	TAGS	DESCRIPTION	MANUFACTURER	PART No.	QTY.
		RAIL-C			
67	X11	FEED THROUGH TERMINAL (WDU 2.5)	WEIDMULLER	1020000000	04 Nos.
68	X20	FEED THROUGH POWER TERMINAL (WDU6)	WEIDMULLER	1020200000	02 Nos.
69	X20	EARTH TERMINAL (WPE 6)	WEIDMULLER	1010200000	01 No.
70	F20	MCB 10A 2P	SCHNEIDER ELECTRIC	24336	01 No.
71	F21 – F24	MCB 6A 1P	HAGER	MW106	04 Nos.
72	X21	FEED THROUGH TERMINAL (WDU 2.5)	WEIDMULLER	1020000000	04 Nos.
73	X12 & X22	FUSE TERMINAL (WSI 6)	WEIDMULLER	1011000000	EACH 06
74		FEED THROUGH TERMINAL (WDU 2.5)	WEIDMULLER	1020000000	EACH 12
		RAIL-D			
75	ES1 & ES2	ETHERNET SWITCH	KORENIEX	JETNET 4510	02 Nos.
76	HAI	ANALOG HART MODULE	PROSOFT	5208 MNET-HART	01 No.
77	MCM1 & MCM2	MODBUS MODULE (MODBUS TO MODBUS)	PROSOFT	5302-MBP-MCM4	02 Nos.
78	K1 – K32	PLUGGABLE RELAY, CR-P024DC2, 2 C/O, 250V, 8A, 24VDC	ABB	1SVR405601R1000	32 Nos.
79		SOCKET, CR-PLS, LOGICAL SOCKET WITH SAFETY ISOLATION	ABB	1SVR405650R0000	32 Nos.
80		SOCKET ACCESSORIES, CR-PH, PLASTIC HOLDER	ABB	1SVR405659R0000	32 Nos.
81		DIODE AND LED, CR-P/M 42V, 6-24VDC, GREEN	ABB	1SVR405652R1000	32 Nos.
		RAIL-E			
82	XDI1 – XDI2	FUSE TERMINAL (WSI 6)	WEIDMULLER	1011000000	EACH 32
83		DISCONNECTOR TERMINAL (WTR 2.5)	WEIDMULLER	1855610000	EACH 32
84	XDO1	FUSE TERMINAL (WSI 6)	WEIDMULLER	1011000000	32 Nos.
85		DISCONNECTOR TERMINAL (WTR 2.5)	WEIDMULLER	1855610000	32 Nos.
		RAIL-F			
86	XDI3 – XDI4	FUSE TERMINAL (WSI 6)	WEIDMULLER	1011000000	EACH 32
87		DISCONNECTOR TERMINAL (WTR 2.5)	WEIDMULLER	1855610000	EACH 32
88	XDO2	FUSE TERMINAL (WSI 6)	WEIDMULLER	1011000000	32 Nos.
89		DISCONNECTOR TERMINAL (WTR 2.5)	WEIDMULLER	1855610000	32 Nos.
		RAIL-G			
90	XDI5	FUSE TERMINAL (WSI 6)	WEIDMULLER	1011000000	32 Nos.
91		DISCONNECTOR TERMINAL (WTR 2.5)	WEIDMULLER	1855610000	EACH 32
92	K33- K48	PLUGGABLE RELAY, CR-P024DC2, 2 C/O, 250V, 8A, 24VDC	ABB	1SVR405601R1000	32 Nos.
93		SOCKET, CR-PLS, LOGICAL SOCKET WITH SAFETY ISOLATION	ABB	1SVR405650R0000	32 Nos.
94		SOCKET ACCESSORIES, CR-PH, PLASTIC HOLDER	ABB	1SVR405659R0000	32 Nos.
95		DIODE AND LED, CR-P/M 42V, 6-24VDC, GREEN	ABB	1SVR405652R1000	32 Nos.
96	XDO3	FUSE TERMINAL (WSI 6)	WEIDMULLER	1011000000	32 Nos.
97		DISCONNECTOR TERMINAL (WTR 2.5)	WEIDMULLER	1855610000	32 Nos.

LEGEND:

- CONSTRUCTION SCOPE
- REVISION CLOUD

2	06.05.18	ISSUED FOR CONSTRUCTION	SJM	JLK	NH	AA	
1	03.04.18	ISSUED FOR APPROVAL	SJM	JLK	NH	AA	
0	12.02.18	ISSUED FOR REVIEW	SAA	JLK	NH	AA	
ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD	

CLIENT

هيئة كهرباء ومياه دبي
Dubai Electricity & Water Authority



P.O. BOX: 564, DUBAI, UAE. TEL: 00971-4-324 4444. FAX: 00971-4-324 4922

PROJECT:
SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA
SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY
IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX - PHASE-2 PLC PANEL GA DRAWING - BOM

DEWA PRJ REF : RFX-2131600072
DEWA PO REF : PO: 3761700080
DEWA DWG. NO.
RFX72-PLC-GAD2

VENDOR



Silvertech

P.O. BOX: 17910, JEBEL ALI, DUBAI, U.A.E
T: +971 (4) 8995000. F: +971 (4) 8995001
www.silvertech-me.com

STME DWG. NO.
PRJ212-PH2-INS-GAD-0001


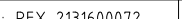
SHEET
09 OF 10

REV.
2

SCALE:
N.T.S.
SIZE:
A3
REV.
2

SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX

GENERAL ARRANGEMENT DRAWING
PHASE-4 PLC PANEL

REFERENCE DRAWINGS/DOCUMENTS:								<div>CLIENT</div> <div><div>هيئة كهرباء ومياه دبي Dubai Electricity & Water Authority</div></div> <div>P.O. BOX: 564, DUBAI, UAE. TEL: 00971-4-324 4444. FAX: 00971-4-324 4922</div>	<div>DEWA PRJ REF : RFX-2131600072 DEWA PO REF : PO: 3761700080</div> <div>DEWA DWG. NO. RFX72-PLC-GAD4</div>	<div>VENDOR</div> <div><div>Silvertech</div><div>طريق جبل علي 17910، دبي، الإمارات العربية المتحدة P.O. BOX: 17910, JEBEL ALI, DUBAI, U.A.E T: +971 (4) 8995000, F: +971 (4) 8995001 www.silvertech-me.com</div></div> <div>STME DWG. NO. PRJ212-PH4-INS-GAD-0002</div> <div>SHEET 01 OF 10</div>	SCALE: N.T.S.
							SIZE: A3				
	1	27.03.18	ISSUED FOR CONSTRUCTION	SJM	JLK	NH	AA				REV. 1
	0	22.02.18	ISSUED FOR REVIEW	SAA	JLK	NH	AA				
	ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD				
	PROJECT: SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX - PHASE-4 PLC PANEL GA DRAWING - COVER SHEET										

PRJ212-PH4-INS-GAD-0002-02

SHEET NO.	DESCRIPTION	FILE NAME	ISSUE	REVISIONS				PURPOSE OF ISSUE
				0	1	2	3	
1	PHASE-4 PLC PANEL GENERAL ARRANGEMENT DRAWING - COVER SHEET	PRJ212-PH4-INS-GAD-0002-01	27.03.18	X	X			ISSUED FOR CONSTRUCTION
2	PHASE-4 PLC PANEL GENERAL ARRANGEMENT DRAWING - INDEX SHEET	PRJ212-PH4-INS-GAD-0002-02	27.03.18	X	X			ISSUED FOR CONSTRUCTION
3	PHASE-4 PLC PANEL GENERAL ARRANGEMENT DRAWING - COMBINED VIEW	PRJ212-PH4-INS-GAD-0002-03	27.03.18	X	X			ISSUED FOR CONSTRUCTION
4	PHASE-4 PLC PANEL GENERAL ARRANGEMENT DRAWING - CPU PANEL	PRJ212-PH4-INS-GAD-0002-04	27.03.18	X	X			ISSUED FOR CONSTRUCTION
5	PHASE-4 PLC PANEL GENERAL ARRANGEMENT DRAWING - I/O PANEL	PRJ212-PH4-INS-GAD-0002-05	27.03.18	X	X			ISSUED FOR CONSTRUCTION
6	PHASE-4 PLC PANEL GENERAL ARRANGEMENT DRAWING - RACK DETAILS	PRJ212-PH4-INS-GAD-0002-06	27.03.18	X	X			ISSUED FOR CONSTRUCTION
7	PHASE-4 PLC PANEL GENERAL ARRANGEMENT DRAWING - BILL OF MATERIAL	PRJ212-PH4-INS-GAD-0002-07	27.03.18	X	X			ISSUED FOR CONSTRUCTION
8	PHASE-4 PLC PANEL GENERAL ARRANGEMENT DRAWING - BILL OF MATERIAL	PRJ212-PH4-INS-GAD-0002-08	27.03.18	X	X			ISSUED FOR CONSTRUCTION
9	PHASE-4 PLC PANEL GENERAL ARRANGEMENT DRAWING - BILL OF MATERIAL	PRJ212-PH4-INS-GAD-0002-09	27.03.18	X	X			ISSUED FOR CONSTRUCTION
10	PHASE-4 PLC PANEL GENERAL ARRANGEMENT DRAWING - BILL OF MATERIAL	PRJ212-PH4-INS-GAD-0002-10	27.03.18	X	X			ISSUED FOR CONSTRUCTION
11								
12								
13								
14								
15								
16								
17								
18								
19								
20								
21								
22								
23								
24								
25								
26								
27								
28								
29								
30								
31								
32								
33								
34								
35								
36								
37								
38								

REFERENCE DRAWINGS/DOCUMENTS:

1	27.03.18	ISSUED FOR CONSTRUCTION	SJM	JLK	NH	AA	
0	22.02.18	ISSUED FOR REVIEW	SAA	JLK	NH	AA	
ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD	

CLIENT

هيئة كهرباء ومياه دبي

Dubai Electricity & Water Authority




P.O. BOX: 564, DUBAI, UAE. TEL: 00971-4-324 4444. FAX: 00971-4-324 4922

DEWA PRJ REF : RFX-2131600072
DEWA PO REF : PO: 3761700080
DEWA DWG. NO.
RFX72-PLC-GAD4

PROJECT:
SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA
SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY
IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX - PHASE-4 PLC PANEL GA DRAWING-INDEX SHEET

VENDOR



Silvertech

شركة سيلفرتيخ

P.O. BOX: 17910, JEBEL ALI, DUBAI, U.A.E
T: +971 (4) 8995000. F: +971 (4) 8995001
www.silvertech-me.com

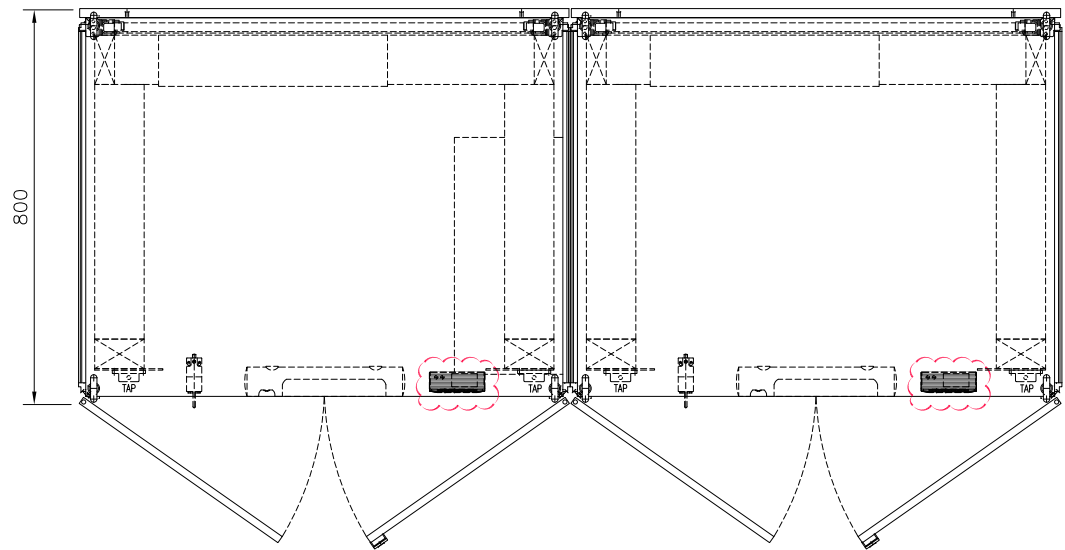
STME DWG. NO.
PRJ212-PH4-INS-GAD-0002

SCALE:
N.T.S.

SIZE:
A3

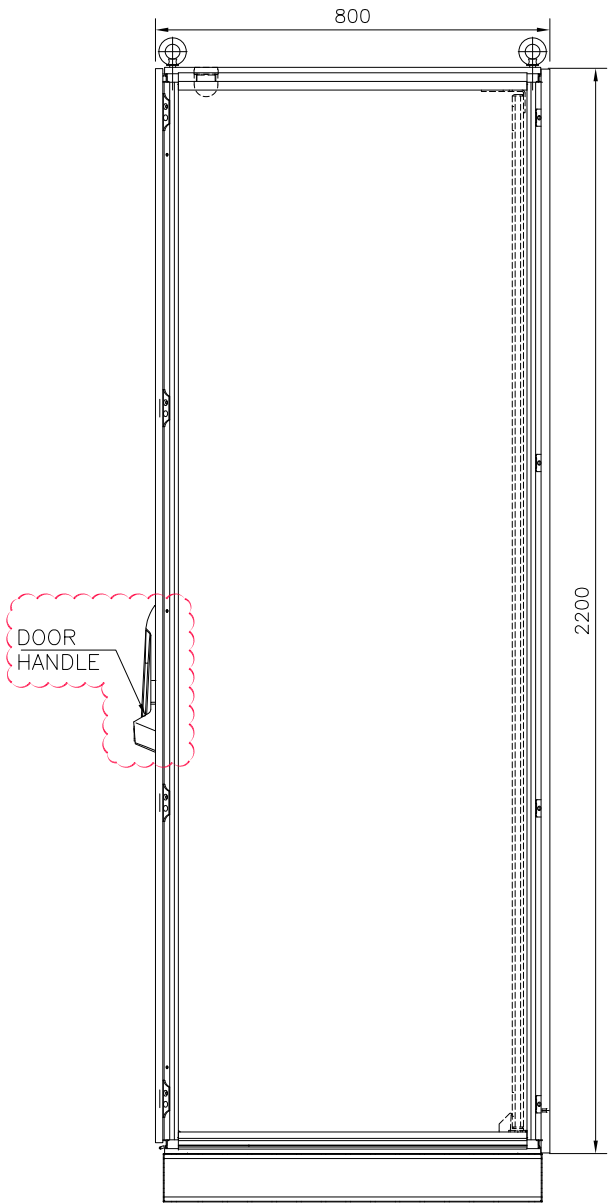
REV.
1

SHEET
02 OF 10

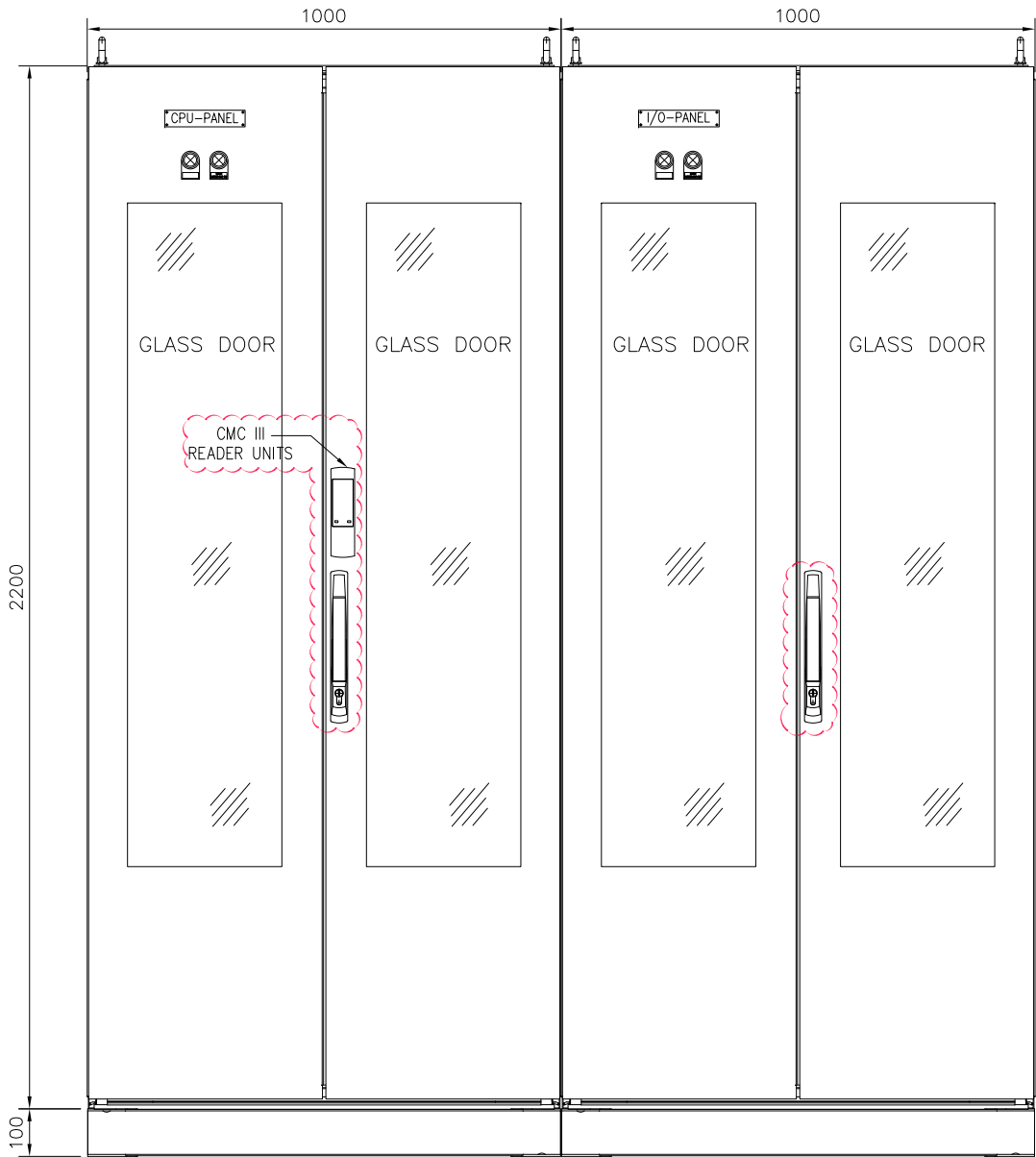


NOTES:

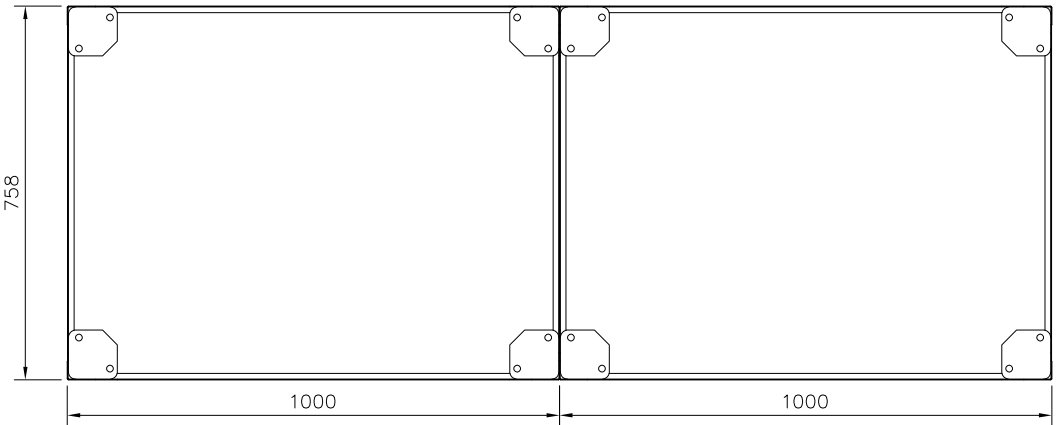
1. L&T ENCLOSURE: (1000W X 800D X 2200H) WITH FRONT DOOR
2. ENCLOSURE FRAME: DIPCOAT PRIMED IN RAL 7035 1.5MM THICK SHEET STEEL.
3. DOORS: DIPCOAT PRIMED AND POWDER AND POWDER COATED IN TEXTURED RAL 7035 2MM THICK SHEET STEEL.
4. ROOF: DIPCOAT PRIMED AND POWDER COATED IN TEXTURED RAL 7035 1.5MM THICK SHEET STEEL.
5. MOUNTING PLATE: ZINC PLATED 3MM THICK SHEET STEEL.
6. PLINTH: RAL 7022 SHEET STEEL.
7. PROTECTION CATEGORY: IP54 TO EN 60529/10.91
8. COMPLIES WITH: NEMA 12
9. CABLE ENTRY & EXIT: BOTTOM.



SIDE VIEW



FRONT VIEW WITH DOOR




PLINTH TOP VIEW

LEGEND:

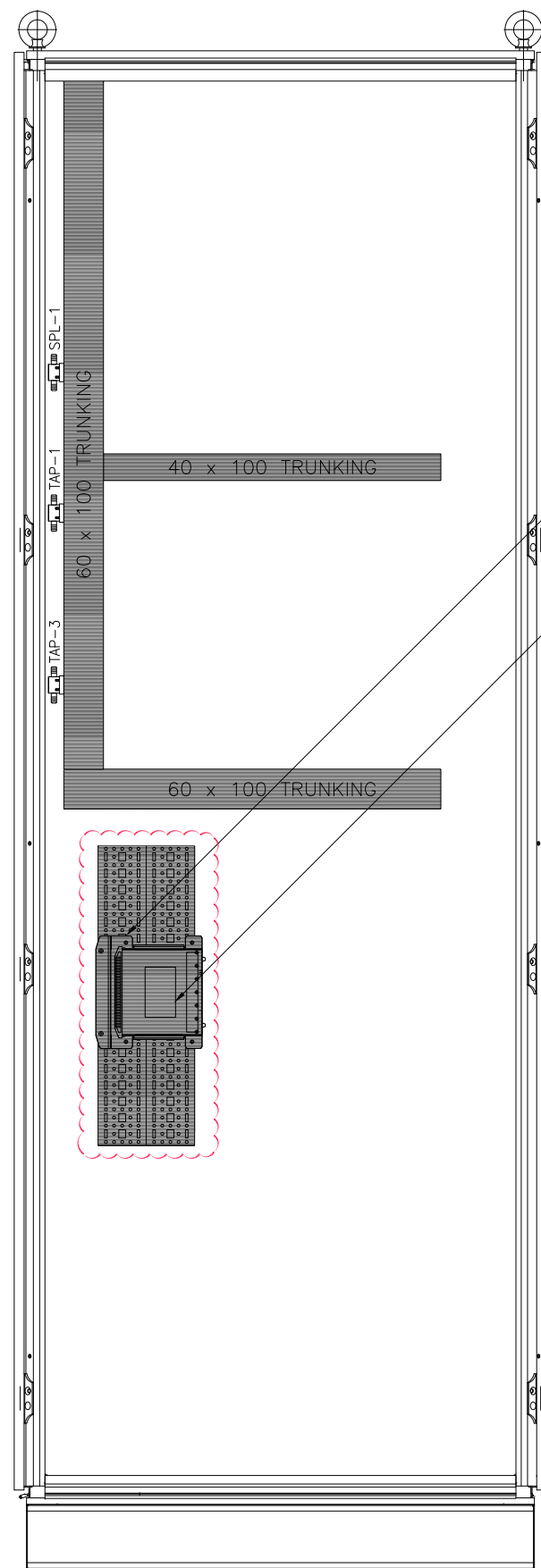
CONSTRUCTION SCOPE

1	27.03.18	ISSUED FOR CONSTRUCTION	SJM	JLK	NH	AA	
0	22.01.18	ISSUED FOR REVIEW	SAA	JLK	NH	AA	
ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD	

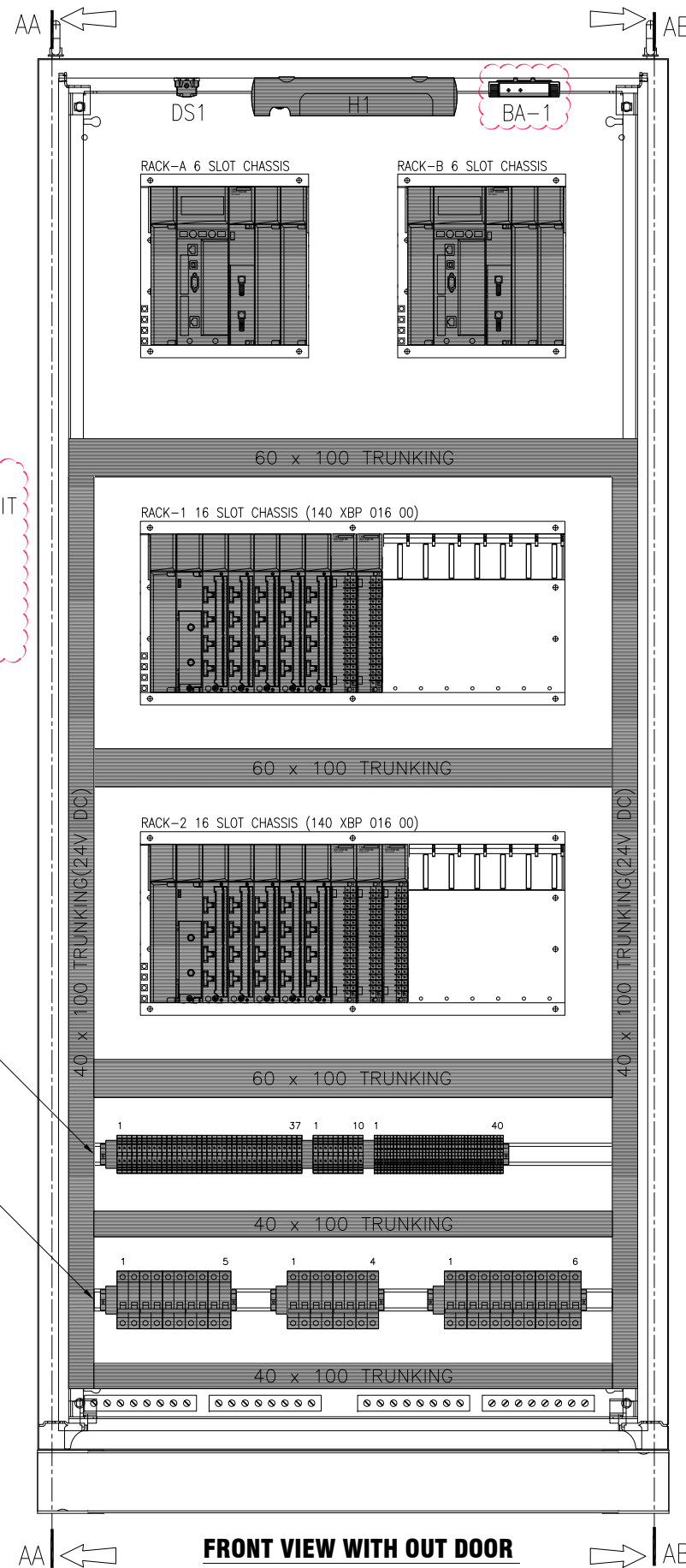
CLIENT	DEWA PRJ REF : RFX-2131600072 DEWA PO REF : PO: 3761700080 DEWA DWG. NO. RFX72-PLC-GAD4
PROJECT:	SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX - PHASE-4 PLC PANEL GA DRAWING-COMBINED VIEW

VENDOR	SCALE:
	1 : 15
P.O. BOX: 17910, JEBEL ALI, DUBAI, U.A.E T: +971 (4) 8995000, F: +971 (4) 8995001 www.silvertech-me.com	SIZE:
STME DWG. NO. PRJ212-PH4-INS-GAD-0002	A3
SHEET 03 OF 10	REV.
	1

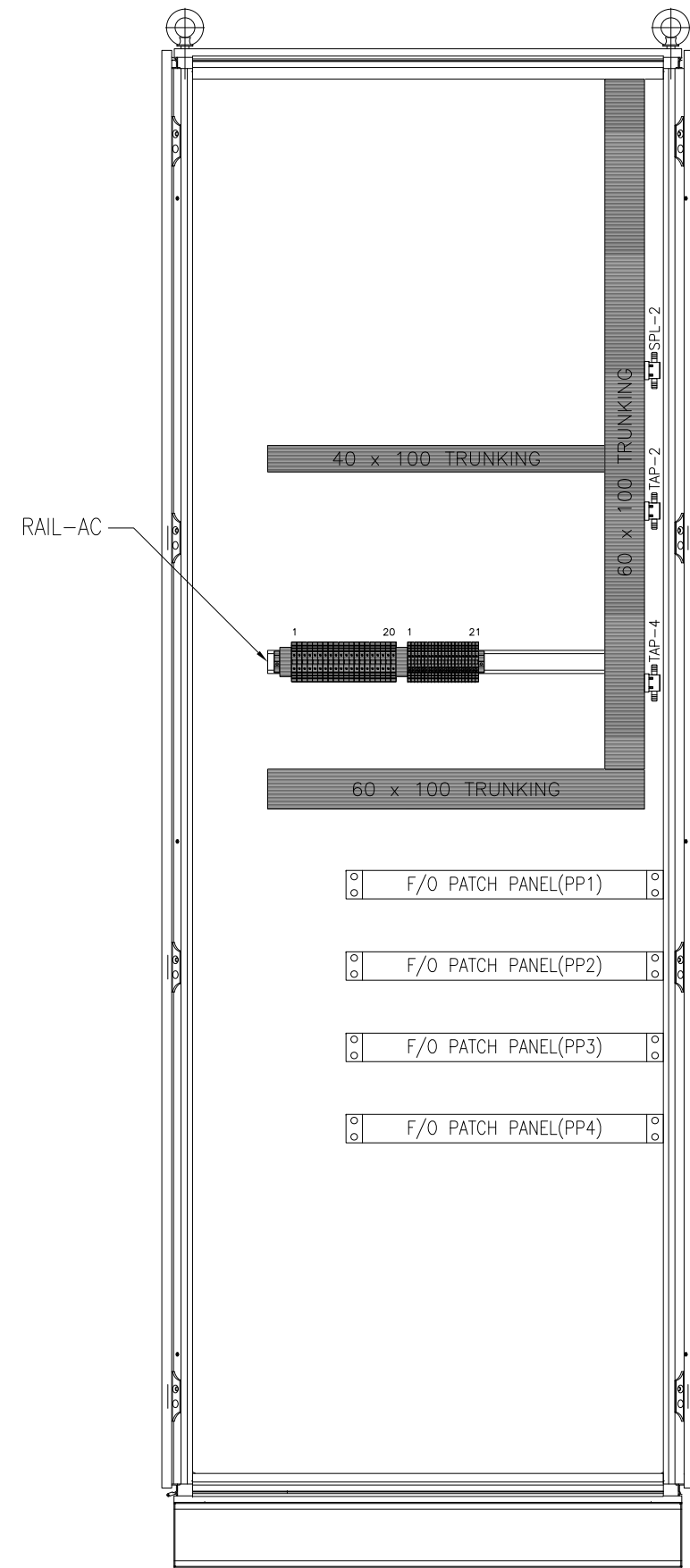
PRJ212-PH4-INS-GAD-0002-04



"AA-AA" VIEW



FRONT VIEW WITH OUT DOOR



"AB-AB" VIEW

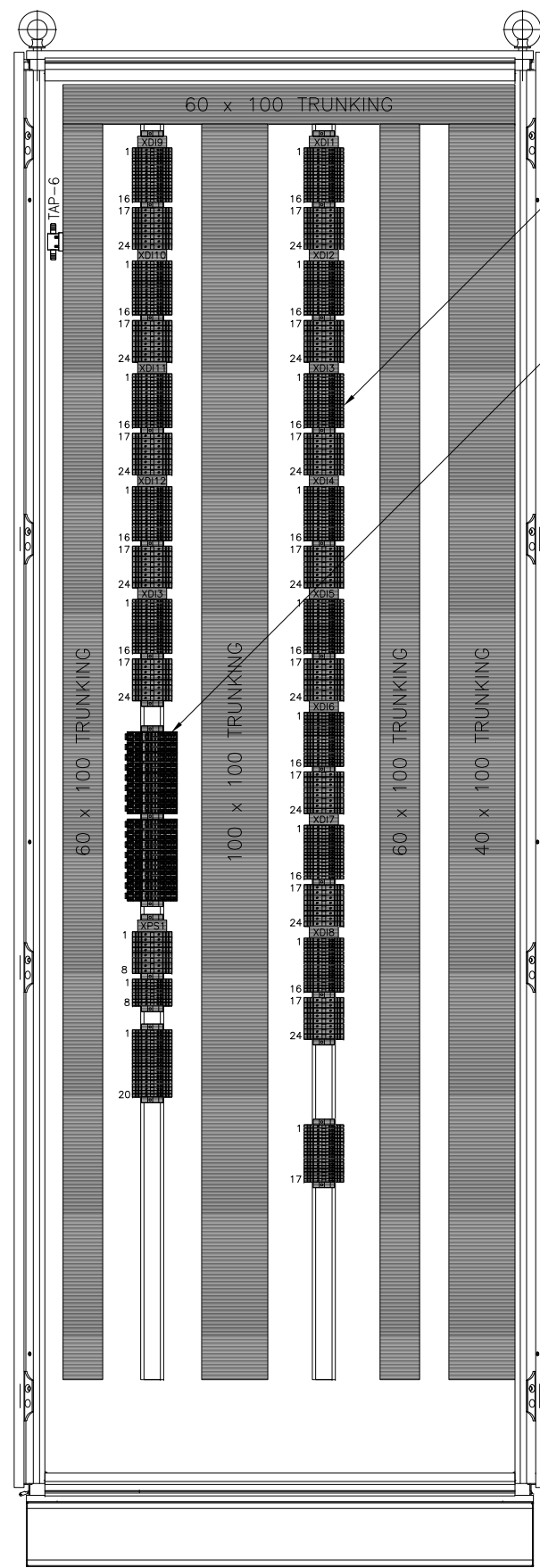
LEGEND:

CONSTRUCTION SCOPE

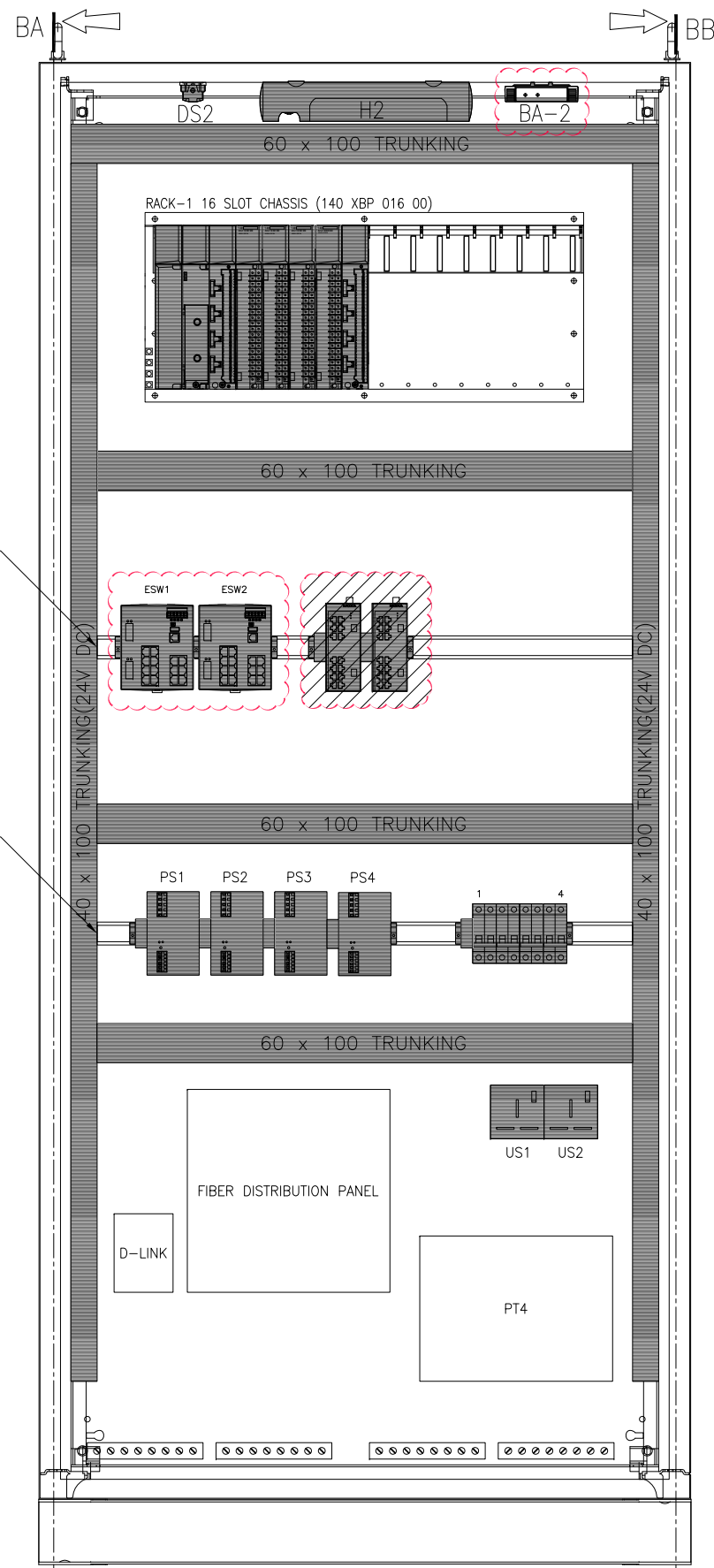
1	27.03.18	ISSUED FOR CONSTRUCTION	SJM	JLK	NH	AA
0	22.01.18	ISSUED FOR REVIEW	SAA	JLK	NH	AA
ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD

CLIENT	DEWA PRJ REF : RFX-2131600072 DEWA PO REF : PO: 3761700080
PROJECT:	DEWA DWG. NO. RFX72-PLC-GAD4
SUPPLY, INSTALLATION, TESTING, COMMISSIONING OF NEW SCADA SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING, NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX - PHASE-4 PLC PANEL GA DRAWING - CPU PANEL	

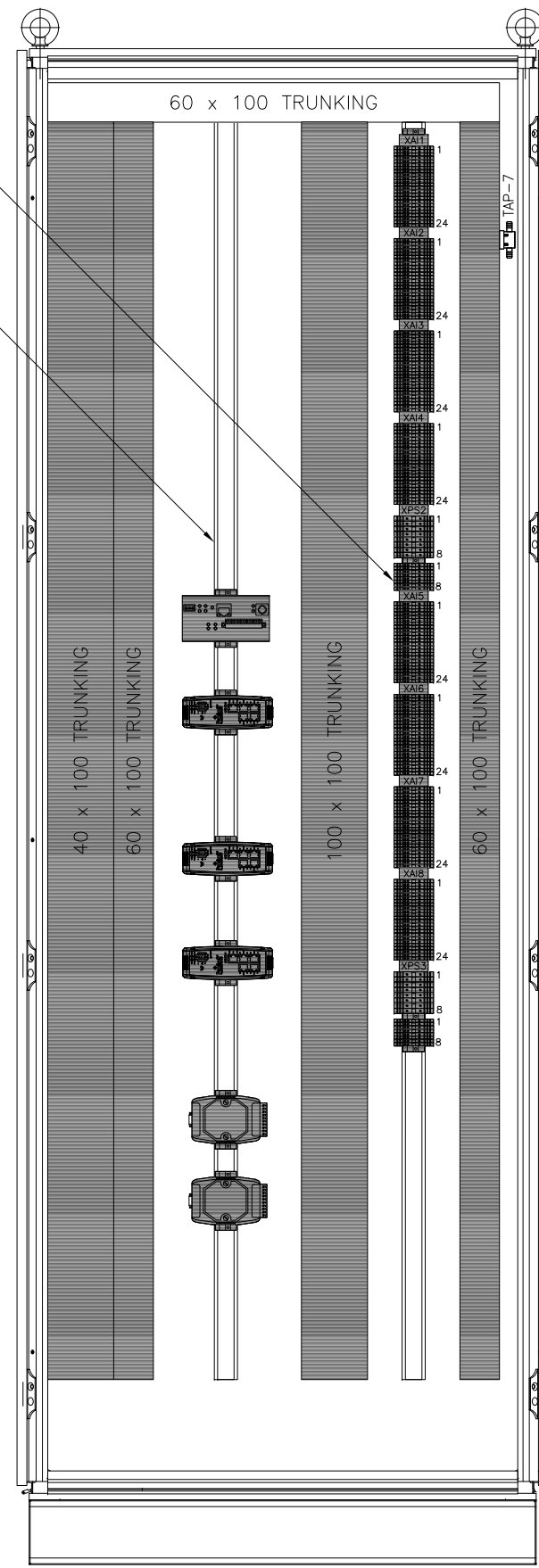
VENDOR	SCALE:
 P.O. BOX: 17910, JEBEL ALI, DUBAI, U.A.E T: +971 (4) 8995000, F: +971 (4) 8995001 www.silvertech-me.com	1 : 10
	SIZE:
	A3
STME DWG. NO.	REV.
PRJ212-PH4-INS-GAD-0002	1
SHEET	
04 OF 10	



"BA-BA" VIEW



FRONT VIEW WITH OUT DOOR



"BB-BB" VIEW

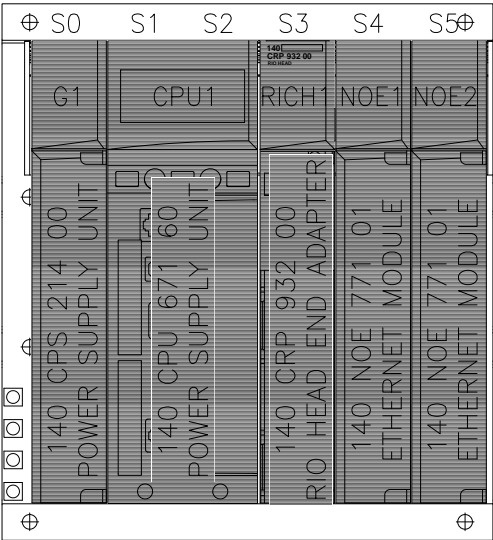
LEGEND:

- CONSTRUCTION SCOPE
- DEMOLITION SCOPE

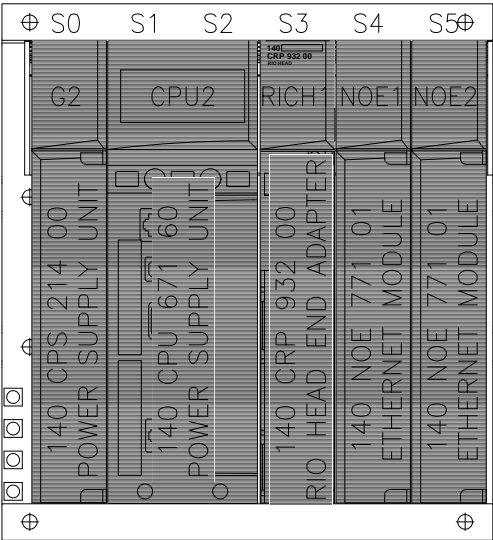
1	27.03.18	ISSUED FOR CONSTRUCTION	SJM	JLK	NH	AA
0	22.01.18	ISSUED FOR REVIEW	SAA	JLK	NH	AA
ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD

CLIENT	DEWA PRJ REF : RFX-2131600072 DEWA PO REF : PO: 3761700080
PROJECT:	DEWA DWG. NO. RFX72-PLC-GAD4
SUPPLY, INSTALLATION, TESTING, COMMISSIONING OF NEW SCADA SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING, NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX - PHASE-4 PLC PANEL GA DRAWING - I/O PANEL	

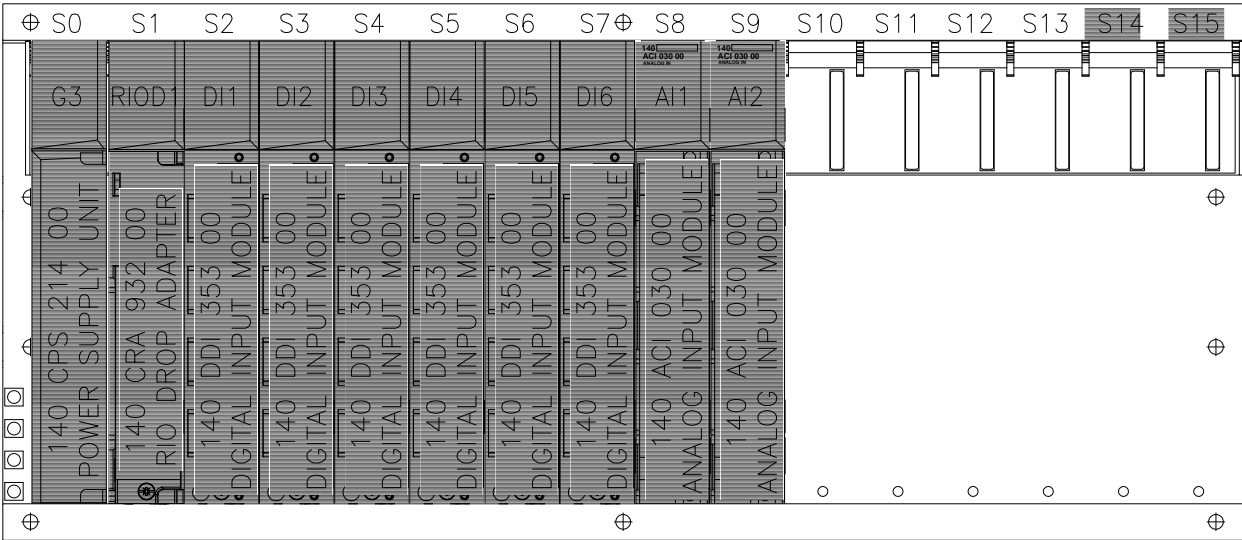
VENDOR	SCALE:
Silvertech	1 : 10
P.O. BOX: 17910, JEBEL ALI, DUBAI, U.A.E T: +971 (4) 8995000, F: +971 (4) 8995001 www.silvertech-me.com	SIZE: A3
STME DWG. NO. PRJ212-PH4-INS-GAD-0002	SHEET 05 OF 10
	REV. 1



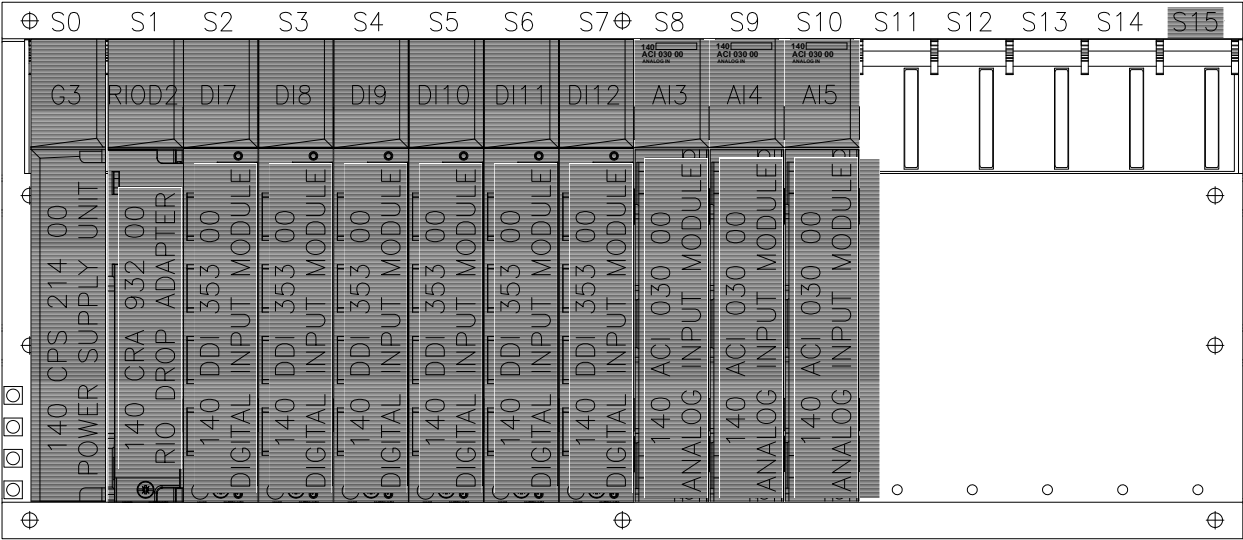
RACK-A 6 SLOT CHASSIS



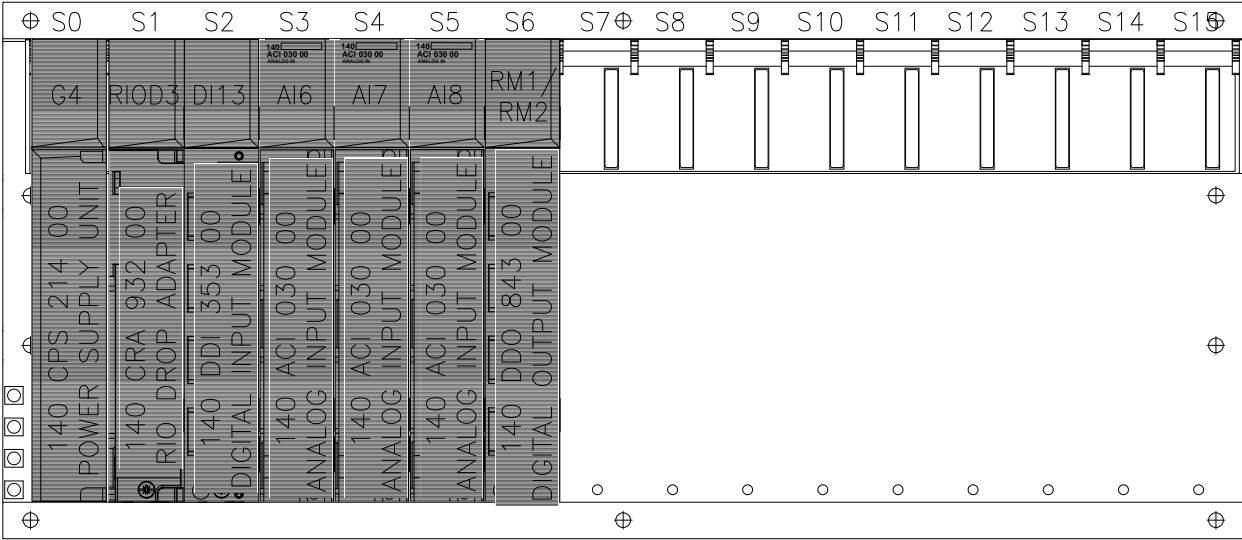
RACK-B 6 SLOT CHASSIS



RACK-1 16 SLOT CHASSIS (140 XBP 016 00)
CPU PANEL



RACK-2 16 SLOT CHASSIS (140 XBP 016 00)
CPU PANEL





RACK-1 16 SLOT CHASSIS (140 XBP 016 00)
I/O PANEL

RACK DETAILS

REFERENCE DRAWINGS/DOCUMENTS:

1	27.03.18	ISSUED FOR CONSTRUCTION	SJM	JLK	NH	AA	
0	22.01.18	ISSUED FOR REVIEW	SAA	JLK	NH	AA	
ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD	

CLIENT <div> هيئة كهرباء ومياه دبي Dubai Electricity & Water Authority</div> <div>P.O. BOX: 564, DUBAI, UAE. TEL: 00971-4-324 4444. FAX: 00971-4-324 4922</div>	DEWA PRJ REF : RFX-2131600072 DEWA PO REF : PO: 3761700080		VENDOR <div> Silvertech P.O. BOX: 17910, JEBEL ALI, DUBAI, U.A.E T: +971 (4) 8995000, F: +971 (4) 8995001 www.silvertech-me.com</div>	SCALE: N.T.S.
	DEWA DWG. NO. RFX72-PLC-GAD4			SIZE: A3
PROJECT: SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX - PHASE-4 PLC PANEL GA DRAWING-RACK DETAILS	STME DWG. NO. PRJ212-PH4-INS-GAD-0002		SHEET 06 OF 10	REV. 1

PRJ212-PH4-INS-GAD-0002-07

SR NO.	TAGS	DESCRIPTION	MANUFACTURER	PART No.	QTY.
		CPU-PANEL			
1	-	ENCLOSURE (800W X 800D X 2200H) WITH FRONT	L&T	-	01 No.
2	DS1	DOOR SWITCH	-	-	01 No.
3	H1	PANEL LIGHT	PHILIPS	-	01 No.
4	-	PANEL PLINTH	-	-	01 No.
5	HL1, HL2	RED COLOR INDICATION LAMP	TEKNIC	2LHLR	02 Nos.
6	-	ERGOFORM-S HANDLE	RITTAL	DK 7320.700	01 No.
7	-	SEMI CYLINDER	RITTAL	SZ 2467.000	01 No.
8	RU-1	CMC III READER UNITS	RITTAL	DK 7030.230	01 No.
9	PU-1	CMC III PROCESSING UNITS	RITTAL	DK 7030.010	01 No.
10	BA-1	CMC III CAN BUS ACCESS	RITTAL	DK 7030.200	01 No.
11	-	CMC III MOUNTING UNIT	RITTAL	DK 7030.071	01 No.
		RACK-A			
12	RACK-A	6 SLOT CHASSIS	MODICON	140 XBP 006 00	01 No.
13	G1	24V DC, RACK POWER SUPPLY UNIT	MODICON	140 CPS 214 00	01 No.
14	CPU1	PROCESSOR UN IT	MODICON	140 CPU 671 60	01 No.
15	RICH1	RIO HEAD END ADAPTER	MODICON	140 CRP 932 00	01 No.
16	NOE1 & NOE2	ETHERNET MODULE	MODICON	140 NOE 771 01	02 Nos.
		RACK-B			
17	RACK-B	6 SLOT CHASSIS	MODICON	140 XBP 006 00	01 No.
18	G2	24V DC, RACK POWER SUPPLY UNIT	MODICON	140 CPS 214 00	01 No.
19	CPU2	PROCESSOR UN IT	MODICON	140 CPU 671 60	01 No.
20	RICH2	RIO HEAD END ADAPTER	MODICON	140 CRP 932 00	01 No.
21	NOE3 & NOE4	ETHERNET MODULE	MODICON	140 NOE 771 01	02 Nos.
		RACK-1			
22	RACK-1	16 SLOT CHASSIS	MODICON	140 XBP 016 00	01 No.
23	G3	24V DC, RACK POWER SUPPLY UNIT	MODICON	140 CPS 214 00	01 No.
24	RIOD1	RIO DROP ADAPTER	MODICON	140 CRA 932 00	01 No.
25	DI1....DI6	DIGITAL INPUT MODULE 32 CHANNEL	MODICON	140 DDI 353 00	06 Nos.
26	AI1....AI2	ANALOG INPUT MODULE 8 CHANNEL	MODICON	140 ACI 030 00	02 Nos.
		RACK-2			
27	RACK-2	16 SLOT CHASSIS	MODICON	140 XBP 016 00	01 No.
28	G4	24V DC, RACK POWER SUPPLY UNIT	MODICON	140 CPS 214 00	01 No.
29	RIOD2	RIO DROP ADAPTER	MODICON	140 CRA 932 00	01 No.
30	DI6....DI12	DIGITAL INPUT MODULE 32 CHANNEL	MODICON	140 DDI 353 00	06 Nos.
31	AI3....AI5	ANALOG INPUT MODULE 8 CHANNEL	MODICON	140 ACI 030 00	03 Nos.

LEGEND:



CONSTRUCTION SCOPE

1	27.03.18	ISSUED FOR CONSTRUCTION	SJM	JLK	NH	AA	
0	22.02.18	ISSUED FOR REVIEW	SAA	JLK	NH	AA	
ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD	

CLIENT



DEWA PRJ REF : RFX-2131600072
DEWA PO REF : PO: 3761700080
DEWA DWG. NO.
RFX72-PLC-GAD4

PROJECT:

SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA
SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY
IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX - PHASE-4 PLC PANEL GA DRAWING - BOM

VENDOR



P.O. BOX: 17910, JEBEL ALI, DUBAI, U.A.E.
T: +971 (4) 8995000, F: +971 (4) 8995001
www.silvertech-me.com

STME DWG. NO.
PRJ212-PH4-INS-GAD-0002

SHEET
07 OF 10

SCALE:

N.T.S.

SIZE:

A3

REV.

1

PRJ212-PH4-INS-GAD-0002-08

SR NO.	TAGS	DESCRIPTION	MANUFACTURER	PART No.	QTY.
32	SPL1 & SPL2	SPLITTER	MODICON	MA 0186 100C	02 Nos.
33	TAP1....TAP4	R I/O TAP	MODICON	MA 0185 100C	04 Nos.
		RAIL-AA			
34	AA-TB01	FUSE TERMINAL	-	-	37 Nos.
35	AA-TB02	FUSE TERMINAL	-	-	10 Nos.
36	AA-TB03	FEED THROUGH TERMINAL	-	-	40 Nos.
		RAIL-AB			
37	PT1	MCB 16A 2P	LS	BKN C16	01 No.
38	Q1....Q4	MCB 10A 2P	HAGER	MV210	04 Nos.
39	Q5	MCB 16A 2P	LS	BKN C16	01 No.
40	Q6, Q12 & Q13	MCB 10A 2P	HAGER	MV210	03 Nos.
41	Q7	MCB 16A 2P	LS	BKN C16	01 No.
42	Q8....Q11 & Q14	MCB 10A 2P	HAGER	MV210	04 Nos.
		RAIL-AC			
43	AC-TB01	FUSE TERMINAL	-	-	20 Nos.
44	AC-TB02	FEED THROUGH TERMINAL	-	-	21 Nos.
45	PP1....PP4	PATCH PANEL	-	-	04 Nos.
46		PATCH CORD	-	-	04 Nos.
		I/O-PANEL			
47	-	ENCLOSURE (800W X 800D X 2200H) WITH FRONT	L&T	-	01 No.
48	DS2	DOOR SWITCH	-	-	01 No.
49	H2	PANEL LIGHT	PHILIPS	-	01 No.
50	-	PANEL PLINTH	-	-	01 No.
51	HL3, HL4	RED COLOR INDICATION LAMP	TEKNIC	2LHLR	02 Nos.
52	-	ERGOFORM-S HANDLE	RITTAL	DK 7320.700	01 No.
53	-	SEMI CYLINDER	RITTAL	SZ 2467.000	01 No.
54	BA-1	CMC III CAN BUS ACCESS	RITTAL	DK 7030.200	01 No.
		RACK-1			
55	RACK-1	16 SLOT CHASSIS	MODICON	140 XBP 016 00	01 No.
56	G5	24V DC, RACK POWER SUPPLY UNIT	MODICON	140 CPS 214 00	01 No.
57	RIOD3	RIO DROP ADAPTER	MODICON	140 CRA 932 00	01 No.
58	DI13	DIGITAL INPUT MODULE 32 CHANNEL	MODICON	140 DDI 353 00	01 No.
59	AI6....AI8	ANALOG INPUT MODULE 8 CHANNEL	MODICON	140 ACI 030 00	03 Nos.
60	RM1/RM2	DIGITAL INPUT MODULE 32 CHANNEL	MODICON	140 DDI 353 00	01 No.

LEGEND:

CONSTRUCTION SCOPE

1	27.03.18	ISSUED FOR CONSTRUCTION	SJM	JLK	NH	AA	
0	22.02.18	ISSUED FOR REVIEW	SAA	JLK	NH	AA	
ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD	

CLIENT

هيئة كهرباء ومياه دبي
Dubai Electricity & Water Authority



P.O. BOX: 564, DUBAI, UAE. TEL: 00971-4-324 4444. FAX: 00971-4-324 4922

DEWA PRJ REF : RFX-2131600072
DEWA PO REF : PO: 3761700080
DEWA DWG. NO.
RFX72-PLC-GAD4

PROJECT:
SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA
SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY
IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX - PHASE-4 PLC PANEL GA DRAWING - BOM

VENDOR



Silvertech

P.O. BOX: 17910, JEBEL ALI, DUBAI, U.A.E.
T: +971 (4) 8995000. F: +971 (4) 8995001
www.silvertech-me.com

STME DWG. NO.
PRJ212-PH4-INS-GAD-0002



SHEET
08 OF 10

SCALE:
N.T.S.
SIZE:
A3
REV.
1



PRJ212-PH4-INS-GAD-0002-09

SR NO.	TAGS	DESCRIPTION	MANUFACTURER	PART No.	QTY.
61	TAP5 & TAP6	R I/O TAP	MODICON	MA 0185 100C	02 Nos.
		RAIL-B A			
62	ES1 & ES2	ETHERNET SWITCH	KORENEX	JETNET 4510	02 Nos.
63	ESW1 & ESW2	16 PORTS ETHERNET SWITCH	SCHNEIDER ELECTRIC	TCSESM163F2C50	02 Nos.
64	UESW1 & UESW2	16-PORT UNMANAGED ETHERNET SWITCHES	MOXA	EDS-316	02 Nos.
		RAIL-B B			
65	PS1....PS4	POWER SUPPLY 230V AC/24V DC 20A	SCHNEIDER ELECTRIC	ABL 4RSM24200	04 Nos.
66	BB-CB01...CB04	MCB 16A 2P	LS	BKN C16	04 Nos.
		RAIL-B C			
67	XDI1....XDI8	FEED THROUGH TERMINAL (2.5)	-	-	EACH 16
68		FUSE TERMINAL	-	-	EACH 08
69	-	FEED THROUGH TERMINAL (2.5)	-	-	17 Nos.
		RAIL-B D			
70	XDI9....XDI13	FEED THROUGH TERMINAL (2.5)	-	-	EACH 16
71		FUSE TERMINAL	-	-	EACH 08
72	BD-RL01...RL08	RELAY	-	-	08 Nos.
73	BD-TB01	RELAY TERMINATION BOARD	-	-	01 No.
74	BD-RL09...RL16	RELAY	-	-	08 Nos.
75	BD-TB02	RELAY TERMINATION BOARD	-	-	01 No.
76	XPS-1	FUSE TERMINAL	-	-	08 Nos.
77		FEED THROUGH TERMINAL (2.5)	-	-	08 Nos.
78		FEED THROUGH TERMINAL (2.5)	-	-	20 Nos.
		RAIL-B E			
79	P-BUS3	MODBUS TCP/IP TO HART ANALOG GATEWAY	PROSOFT	5208-MNET-HART	01 No.
80	-	TCP/IP TO MODBUS	PROSOFT	PLX31-MBTCP-MBS4	03 Nos.
81	-	CONVERTER	ICP CON	7520AR	02 Nos.
		RAIL-B F			
82	XAI1...XAI4	FEED THROUGH TERMINAL (2.5)	-	-	EACH 24
83	XPS-2	FUSE TERMINAL	-	-	08 Nos.
84		FEED THROUGH TERMINAL (2.5)	-	-	08 Nos.
85	XAI5...XAI8	FEED THROUGH TERMINAL (2.5)	-	-	EACH 24
86	XPS-3	FUSE TERMINAL	-	-	08 Nos.
87		FEED THROUGH TERMINAL (2.5)	-	-	08 Nos.

LEGEND:

-  CONSTRUCTION SCOPE
-  DEMOLITION SCOPE

1	27.03.18	ISSUED FOR CONSTRUCTION	SJM	JLK	NH	AA	
0	22.02.18	ISSUED FOR REVIEW	SAA	JLK	NH	AA	
ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD	

CLIENT <div> Dubai Electricity & Water Authority</div> P.O. BOX: 564, DUBAI, UAE. TEL: 00971-4-324 4444. FAX: 00971-4-324 4922	DEWA PRJ REF : RFX-2131600072 DEWA PO REF : PO: 3761700080	<div> P.O. BOX: 17910, JEBEL ALI, DUBAI, U.A.E T: +971 (4) 8995000. F: +971 (4) 8995001 www.silvertech-me.com</div>	SCALE: N.T.S.	
	DEWA DWG. NO. RFX72-PLC-GAD4		SIZE: A3	
PROJECT: SUPPLY , INSTALLATION , TESTING , COMMISSIONING OF NEW SCADA SYSTEM ALONG WITH PHASE 11 PLC RE_ ENGINEERING , NETWORK SECURITY IMPLEMENTATION AT NAJMA PUMPING STATION COMPLEX - PHASE-4 PLC PANEL GA DRAWING - BOM		STME DWG. NO. PRJ212-PH4-INS-GAD-0002	SHEET 09 OF 10	REV. 1

PRJ212-PH4-INS-GAD-0002-10

SR NO.	TAGS	DESCRIPTION	MANUFACTURER	PART No.	QTY.
88	US-1 & US-2	UTILITY SOCKET WITH SWITCH	-	-	02 Nos.
89	-	D-LINK	-	-	01 No.
90	-	FIBER DISTRIBUTION PANEL	-	-	01 No.
91	-	PT4	-	-	01 No.

LEGEND:

1	27.03.18	ISSUED FOR CONSTRUCTION	SJM	JLK	NH	AA	
0	22.02.18	ISSUED FOR REVIEW	SAA	JLK	NH	AA	
ISSUE	DATE	DESCRIPTION	DD	DOS	CHKD	APRVD	

CLIENT

هيئة كهرباء ومياه دبي

Dubai Electricity & Water Authority

P.O. BOX: 564, DUBAI, UAE. TEL: 00971-4-324 4444. FAX: 00971-4-324 4922

DEWA PRJ REF : RFX-2131600072

DEWA PO REF : PO: 3761700080

DEWA DWG. NO.

RFX72-PLC-GAD4

VENDOR

Silvertech

P.O. BOX: 17910, JEBEL ALI, DUBAI, U.A.E

T: +971 (4) 8995000. F: +971 (4) 8995001

www.silvertech-me.com

STME DWG. NO.

PRJ212-PH4-INS-GAD-0002

SHEET

10 OF 10

SCALE:

N.T.S.

SIZE:

A3

REV.

1

STME/DOP/001, REV-0